

# 计算机网络安全中防火墙技术的应用探索

任蕾蕾

江西省电子信息工程学校 江西南昌 330096

**摘要:** 本文主要研究了在计算机网络整体安全设计中广泛应用的新型防火墙技术和应用方案。通过全面分析防火墙技术系统的安全特点分析和重要性, 针对我国计算机网络运行和建设过程中可能出现的各种技术安全应用问题, 研究相应的防火墙技术系统应用的有效措施, 以提高各种防火墙技术系统安全应用系统的综合有效性, 保证中国计算机网络的整体运行质量。

**关键词:** 计算机; 网络安全; 防火墙技术

## Application exploration of firewall technology in computer network security

Ren Leilei

Jiangxi Electronic Information Engineering School, Nanchang, Jiangxi, 330096

**Abstract:** This paper mainly studies the new firewall technology and application scheme which is widely used in the overall security design of computer networks. Through a comprehensive analysis of the security characteristics and importance of the firewall technology system, in view of various technical security application problems that may occur in the operation and construction of my country's computer network, the effective measures for the application of the corresponding firewall technology system are studied to improve various firewall technologies. The comprehensive effectiveness of the system security application system ensures the overall operation quality of China's computer network.

**Keywords:** computer; network security; firewall technology

### 引言:

科技进步、科学发展技术和实用创新的生产技术, 无论是在城市生产领域, 生活娱乐和食品领域, 都给广大群众带来了极大的便利。但同时, 由于计算机网络技术将成为人类的另一把双刃剑, 同时, 其极大的便捷性也制约了人们信息资源交流、信息共享的实现和经济利益信息分享的实现。还有一些安全风险可能直接导致恶意盗窃机密数据信息和个人信息泄露。不仅影响到未来的环境和整个计算机网络安全, 这也必然会直接影响到国内大量的企业, 由于自身信息安全生产经营管理等一系列因素的影响, 安全问题将产生极其巨大而难以估量的破坏性影响。这对中国网络的安全发展环境是非常严重和不利的, 因此有必要尽早应用科学、安全、有效的网络防火墙技术体系来解决这一问题。

### 1 计算机网络主要的安全问题

#### 1.1 数据安全性威胁

在各类计算机网络工程项目的维护和建设等运行服务过程中, 由于技术水平对网络运行维护的综合影响, 以及业务人员自身的网络专业能力素质, 在入侵防护和检测等各种网络技术的基础工作中, 需要处理两个极端情况, 即连接不足和严重错误。这也会使您的基础设施结构的特定业务建设和操作流程更容易转化为特定的工作流程。这些基础设施因素的组合如果不符合完全合理的物理结构或操作规范, 很容易威胁到整个网络信息系统基础数据的安全水平。同时, 由于客户对自己数据库操作的判断不能充分、合理地执行操作指令, 进而出现数据安全和泄露的问题, 计算机数据库操作指令管理服务人员会随时产生操作错误。与此同时, 随着时间的推移, 一些不法之徒可能会受到经济利益和诱惑条件的诱惑。我们可能会尽力强行进入或攻击公司计算机中设置的各种安全计算机网络, 造成大量涉嫌人员泄露、客户信息被盗等安全网络事故, 影响公司工作活动的有序顺

利进行。

### 1.2 外力因素影响

外力因素可以简单分为自然因素和人为因素。计算机网络中的一般系统是指由各种主要硬件设备组成的系统和由各种次要软件设备组成的系统的两个重要组成部分组成的完整网络。不同的硬件和软件设备之间的连接可能会导致不同系统中的各种硬件和软件设备的安全使用出现可靠性问题等各种因素。硬件设备受其他环境因素的影响,如工作环境、现场条件、老化环境等。一些黑客组织,以及国内一些著名企业对手,往往选择通过邮件群发或他们携带的其他形式的病毒文件,将病毒直接传播给计算机网络用户或属于自己公司的一些内部或计算机网络设备系统。由于此类病毒文件具有系统隐蔽性、潜伏期长、爆发和传播过程快速复杂、跨网络、跨传播渠道分布广泛等致命特点,企业系统人员很难确保在发生大规模疫情时,能够准确、及时、有效应对相应的有针对性的危机。当参与网站安全操作部门的人员仅仅因为重视网站的安全性或者因为对网站的掌握程度或相对缺乏掌握程度等信息安全问题,而点击或打开一个页面,进入一个相对不知名的网站或链接时,也会出现安全问题。影响社会计算机网络的安全性。

### 1.3 周边环境威胁

毕竟计算机网络是另一种可共享性信息存储网络,不同的工作时间、不同的生活地点会产生大量的信息文件和信息数据,可能会出现在各种计算机网络平台上,这自然会增加计算机网络平台安全管理和维护的难度。有的为了企业利益和其他特殊要求,在公共网络服务器上任意发布、传播企业信息和各种涉及个人隐私、企业计算机网络维护的不良信息,严重影响企业计算机网络建设的顺利、安全运行,导致企业信息泄露、内部机密信息泄露等信息安全问题。

## 2 计算机网络中应用防火墙技术的重要性

### 2.1 记录计算机网络中的数据

数据对计算机网络技术建设和普及,对国家计算机网络基础设施的安全稳定具有重要作用。通过网络防火墙系统记录整个计算机网络正常运行和管理所涉及的所有数据以及网络信息的访问记录。能够确保在互联网上及时和有效地综合分类或分组所有类型的计算机数据资料,发现可能含有网络安全风险威胁因素的计算机数据信息,及时进行分析,提出合理有效的措施,及时预防和解决有关问题,避免因网络数据访问困难而影响个人计算机网络数据安全。同时,通过对防火墙记录

的异常数据信息进行整理和汇总,可以快速总结不同网络类型异常数据记录的基本特征,在此基础上进行计算机网络风险的预防、监测和预警。

### 2.2 控制访问特殊网站

在计算机网站的实际运行和管理中,许多网络安全问题都是由网络站点和其他操作操作人员造成的。这类企业网站本身面临的网站系统风险因素比较高,用户点击登录并点击进入相关的网站页面,在登录时也会出现一系列的网络系统问题,影响到网络企业的日常维护运营和整体的稳定性和安全性。介绍防火墙技术,我们可以进行更准确和有效的远程监控,以及一些特殊的安全访问网站操作,如保护用户访问网站的权利。在引入防火墙技术后,我们会考虑相关的安全防护措施,然后由相关的企业运营者和维护人员实施一些后续的安全防护措施,如用户访问和浏览。这本身就可以帮助企业进一步提高网络维护、网络用户访问等工作的整体安全性水平,对整个过程具有相当大的参考使用意义。

### 2.3 及时控制不安全服务

在计算机网络的运行和管理过程中,仍然存在着相当多的潜在的计算机计算机不安全信息服务,这极大地制约了企业计算机运行的发展。通过充分利用防火墙技术,可以将服务器在实际运行中遇到的网络安全风险损失迅速降低到最低限度,可以及时、准确地使用内部防火墙系统进行服务拦截攻击等防护工作,避免外部非法服务器攻击客户的内部网站系统和其他服务。在防火墙系统控制环境下,可以安全地开展各项相关工作,特别是在确保安全、稳定、可靠的运行安全的前提下,实现内外网系统实时数据的交换和监控。

## 3 防火墙技术的主要特点

### 3.1 阻塞通信

防火墙技术可以作为抵御内部传递信息传输和外部信息传输攻击的主要屏障,在外部信息攻击的内部传输中发挥着重要作用,可以更有效地保障内部信息系统的信息安全性。通过使用内部防火墙软件,对各类信息进行自动分析整理和信息传输分析工作,可以进一步提高网络安全信息数据库管理质量的质量,即自动过滤出不符合内部安全规范要求的信息,确保用户内部各类网络环境的安全。

### 3.2 保护用网安全

科学技术水平的飞速发展正成为科学技术发展的三大标志之一,随着信息流的快速增长,很容易受到互联网爆炸的强烈影响。在当前形势下,人们自身的生产生

活行为很容易受到网络环境中诸多不安全因素的影响,从而导致各种计算机网络行为以及网络本身的安全运行。将防火墙协议引入网络后,利用防火墙协议及时、准确地进行网络安全信息发布的认证、验证和评估等技术工作。在网络防火墙技术推动全球人民使用的安全信息几乎百分之百安全、无误之后,人们将能够在此基础上直接过滤筛选信息,这对于有效提高互联网信息传输的安全性和质量,保护互联网信息安全的实际使用具有重要的社会意义。

### 3.3 层次性

根据安全性分析评估指标,防火墙系统将不同类型的网站的安全信息划分为三种不同的防护等级,并对一些不良网站类型和计算机病毒、计算机病毒恶意网站类型的网站进行标记和显示,以有效防止此类网站被用于某些重要目的。

## 4 计算机网络安全中的防火墙技术应用

### 4.1 在访问策略中的应用

访问过滤策略技术是保证计算机网络健康运行的重要组成部分,对人们计算机的远程上网和安全操作有着十分重要的影响。一般来说,在正确认识各种计算机的特点并对其进行科学、严格的分类之后,我们应该考虑应用防火墙技术来进行优化配置管理等基础工作。

典型的防火墙技术介绍及其在网络信息系统安全、设备配置监控、工作环境等方面的应用可分为以下几个基本技术方面。首先,在计算机网络信息系统中,经常会有大量来自不同类型网络单元的信息安全相关信息,防火墙技术的应用也是计算机网络信息系统之间信息类型自动分类的另一个基本目的。在这个以技术基础上,防火墙技术往往能够自动和智能地对这种不同类型的信息以及它们之间产生的相关信息进行重新分类和存档,从而将它们的信息重新分类为具有不同安全类型的多个安全信息单位。根据信息单位性质的要求和用户网络信息应用系统的特点,系统防火墙的要求是不同的。防火墙技术公司也会做出一些有针对性的技术选择,他们的产品也会进行防火墙内部安全保护机制设计和防火墙外部的安全防护,尽可能通过技术与安全防范方法相结合的方法,最终实现并降低用户网络信息的单向传递所带来的潜在网络危险性。第二个,防火墙技术本身进行实时自动分析,了解不同类型网站的网络安全问题的一些实时信息。防火墙技术在对网络安全情况进行初步研究后,结合计算机网络环境中的一些网络特性进行实时自动分析,从而采取更有针对性的实时网络实时安

全策略,从而提高整个计算机网络站点运行的网络实时安全系统的整体运行和安全效率。第三,随着基于个人计算机系统平台的网络技术的发展和更新,计算机的实际系统操作或使用也意味着很容易同时产生大量的网络系统漏洞补丁和补丁,而网络防火墙技术可以更准确、更有效地检测和发现这些漏洞的具体问题,促进这些漏洞更快、更及时地得到解决。

### 4.2 在日志监控中的应用

计算机网络数据库管理系统服务器的日志文件和信息记录包含或记录了计算机网络数据库信息稳定运行或开发维护过程中积累的大量其他计算机网络数据库信息。一般来说,计算机软硬件和软件工作人员在日常维护和运行管理中,难免会遇到大量的运行数据。这也是一个非常、非常大和复杂的管理工程,以管理彻底和仔仔细细审查这大量随机数据中随机生成的数据的计算机操作数据日志所带来的压力。同时由于它往往会无形地浪费人们大量的时间和精力,浪费宝贵的时间,影响整个软硬件和软件的正常运行和工作程序的正常平稳有序地开展。通过防火墙技术平台系统的综合应用,采用最先进、最完善的防病防治防毒技术,通过系统实现三种有效的病毒防控方法,即事前实时预防、事中实时控制和事后病毒防控,通过设置不同类型的病毒程序编码,可以实现远程监控和系统日志管理安全的双重目的。当防火墙网络管理系统自动检测到或出现含有日志数据库信息的计算机网络现象或黑客恶意攻击入侵等情况时,防火墙数据库系统也可以自动立即进行处理。这样可以减少防火墙日志、监控中心数据库日志等异常记录的同时分析和处理的难度。在未来的网络安全应用管理中,提高我国社会计算机网络系统安全管理平台和综合网络系统的安全管理水平,便于用户根据自身需求灵活配置和操作,实现各种安全技术的应用具有重要意义。

### 4.3 在安全配置中的应用

一般来说,防火墙会计算机网络计算机网络的重点区域采取专业性的保护措施,防范各种不良信息,创造安全的计算机网络运行环境。为了确保这类工作能够按计划有序进行,一般建议对安全配置进行升级。防火墙技术在安全配置中的重要应用是信息追踪,在自动监控的基础上,可以及时对不良IP地址进行跟踪,找出不良信息的来源,并在后续工作中进行各种防御操作,安全性得到了显着提高。

### 4.4 防火墙技术中的身份验证和加密技术

除了上述在执行特定的信息加密技术链接方面的例



子外, 防火墙技术的应用还有许多其他的安全应用。经过身份认证和安全验证, 可以帮助通信用户在加密信息通道平台上进行加密信息通信和共享, 不仅成功实现了保护加密通信隐私的重要目的, 还有效提高了安全通信数据的真实安全性。在防火墙技术体系中应用加密技术, 可以有效地保护网络信息, 避免在网络信息的实际传输和使用中出现恶意篡改和加密的问题, 减少数据信息使用引起的病毒攻击的爆发。

## 5 结论

防火墙技术本身可以说是网络安全和网络安全技术的各种完全不同的表现形式, 其网络安全与计算机网络设备运行安全、过程控制安全等具体应用的研究成果也会越来越多样化。平时要特别注意加强微机防火墙技术和应用方法的宣传和培训, 提高站长等计算机维护和

操作人员的业务水平。及时学习和引进新型技术、新的新型计算机防火墙技术和应用方法; 加强计算机系统保护, 安全国家计算机信息网络安全正常有效运行, 监督检查计算机网络系统的正常运行, 推动重大计算机网络系统网络安全突发事件和网络问题的及时预防和解决, 以综合安全的运行环境条件提高我国计算机网络系统的安全性。

## 参考文献:

- [1]廖登, 饶博翰. 计算机网络安全中的防火墙技术应用研究[J]. 福建质量管理, 2018(5): 266.
- [2]张静. 计算机网络安全中的防火墙技术分析[J]. 大陆桥视野, 2017(12): 211-212.
- [3]张雪. 计算机网络信息安全及防护策略浅述[J]. 电脑迷, 2016(9): 86.