ISSN: 2661-3719(Print); 2661-3727(Online)

# 计算机网络安全中防火墙技术的应用与探索

蒋黎黎
云南电信公众信息产业有限公司　云南昆明　650100

**摘　要：**自从计算机面世以来，给人们的生活和生产发展带来了诸多的便利，但计算机网络安全问题也随之而来。面对网络的威胁，人们需要在计算机网络安全中心应用防火墙技术。防火墙技术在实际运用中，可以保护计算机运行的安全、保护人们财产等信息的保密安全等。因此，充分发挥其作用，已逐渐成为一项重要的探索内容。基于此，本文首先针对防火墙技术的相关概念展开简要的阐述，并将其作为切入点，对防火墙技术在计算机网络安全中的实践运用策略展开深入、细致的分析。
**关键词：**计算机；网络安全；防火墙技术

# Application and exploration of firewall technology in computer network security

Lili Jiang
Yunnan Telecom Public Information Industry Co., Ltd. Kunming, Yunnan 650100

**Abstract:** Since the advent of the computer, it has brought a lot of convenience to people's life and production development, but the problem of computer network security has also followed. Facing the threat of the network, people need to apply firewall technology in computer network security centers. In practice, firewall technology can protect the security of computer operations and the confidentiality of people's property and other information. Therefore, giving full play to its role has gradually become an important exploration content. Based on this, this paper first briefly expounds on the related concepts of firewall technology and takes it as a starting point to carry out an in-depth and detailed analysis of the practical application strategy of firewall technology in computer network security.
**Keywords:** computer; Network security; Firewall technology

## 引言：

计算机网络安全性的提升，是保障用户数据信息传输安全、避免黑客等不法攻击的重要途径。为达到这一目的，相关研究人员开展了持续而深入的研究，研发出了多种有效保障计算机网络安全的方式及策略。其中防火墙技术是具有代表性且效果突出的防护技术之一，它的运用能够将数据信息进行安全隔离，为信息数据在储存、传输、使用等过程中建立了一道防护屏障，实现了对网络攻击、携带病毒的数据的过滤与隔绝，同时还能在计算机运行过程中对计算机网络的安全情况进行实时监督，更有效地保障了数据信息的安全。防火墙技术一直以来都在计算机网络安全中发挥着出色作用，在网络安全保障需求不断提升的时代中应得到更广泛的运用。

## 一、防火墙技术的相关概念阐述

通俗而言，在内部专用网络、公共网络之间建立起一个安全维护屏障是防火墙技术的最大用途，能够起到信息与数据过滤的作用，促使公共网络当中有可能会影响到内部专用网络安全的数据、信息找寻并作出清除，如此，大幅度的将计算机网络安全系数提高。针对于防火墙技术而言，通常由四个部分组成，即身份验证用具、访问服务相关政策、网络的高效运用以及数据信息的过滤。充分在计算机网络当中运用防火墙技术，可以将人民群众的财产与个人信息展开维护，促使其使用计算机

**个人简介：**蒋黎黎，1986年9月19日，女，汉，四川，安全工程师，云南电信公众信息产业有限公司，资深安全工程师、高级项目经理，本科，信息安全、网络安全，邮箱：13398850919@189.cn。

网络期间，能够始终处于安全的环境下。

## 二、防火墙的分类

1.网络级防火墙

通过或失败通常根据每个IP数据包的源地址和目标地址、应用程序、协议和端口来判断。防火墙检查每个规则，直到数据包信息与特定规则一致。当没有需要满足的规则时，防火墙使用基本规则。通常，基本规则是防火墙要求丢弃数据包。通过基于TCP或UDP数据包定义端口号，防火墙可以决定是否允许特定连接，如Telnet和FTP。

2.电路级网关

在受信任的客户端或服务器和不受信任的主机之间使用TCP握手信息确定会话是否合法。电路级网关过滤OSI模型会话层中的数据包。过滤防火墙必须有两层以上。线路级网关代理服务器功能代理服务器是防火墙网关中设置的一种特殊的应用级代码。通过此代理服务，网络管理员可以允许或拒绝特定应用程序或应用程序的特定功能。数据包过滤技术和应用网关使用特定逻辑来决定是否允许特定数据包通过，从而成功隔离防火墙内外的计算机系统。

3.应用级网关

应用级网关可以检查传入和传出的数据包，并通过网关复制和传输数据，因此可以防止可靠的服务器、客户端及不可靠的主机之间的直接连接。应用层网关可以理解应用层中的协议，执行更复杂的访问控制，以及准确地注册和审核。对于一种特殊的网络应用服务协议，即数据过滤协议，可以分析数据包并编写相关报告。应用程序网关提供对特定环境的严格控制，以方便登录、控制所有输入和输出通信，并防止有价值的程序和数据被盗。

4.分级防火墙

分级防火墙是分布式防火墙的进一步完善，分布式防火墙最大的特点是解决了传统防火墙中单失效点和流量瓶颈等多种问题，但是其自身也存在一些弱势，如因为整个网络的安全性无法保障，所以在使用的过程中会存在一些不便，因此，人们在其基础上研制出了分级防火墙。分级防火墙的主要优势是一级防火墙可以隐藏内部网络的拓扑结构；下级防火墙可以对上一层分流下来的数据信息进行深度的过滤，并且还可以提升整个防火墙的功能，保障内部数据信息的安全性。此外，分级防火墙还可以把安全策略细化，为不同的用户提供不同的需求。

## 三、计算机网络安全发展现状

计算机网络存在很多看不见的安全隐患，这是由于计算机网络开放性特点造成的问题，无法避免会面对不法分子的侵袭，尤其是各类公共场所，由于安全防护措施不到位，会被当做主要的入侵目标。虽然计算机网络发展十分迅速，但其中仍存在不完善之处，尤其在网络安全方面，是当下最需要注重的问题。一般来说计算机网络存在安全漏洞，就会导致出现病毒感染等安全风险，很多不法分子会利用电脑病毒，入侵用户的计算机网络，例如2006年出现的网络病毒熊猫烧香，这款病毒正是湖北李俊打造的一款蠕虫病毒，当年网络已经大量普及，中毒用户不计其数，全国估计数百万计算机中毒，而且这个病毒的变种数量竟然接近100种，并且拥有自动传播、自动感染硬盘的能力，不仅能够感染系统中的exe、com、pif、asp等文件，还能终止反病毒软件进程，让用户遭受了较大的经济损失。

## 四、计算机网络安全中防火墙技术的实践应用

1.定时对病毒库更新并加强病毒的控制功能

针对于计算机网络而言，存在大量的信息与数据，所以，非常容易遭受到各种形式、各种类型的病毒入侵，会将使用者的个人与财产数据、信息盗取，严重影响到使用者的个人权益。另外，在使用单位当中，一个设备的计算机网络如果存在病毒的入侵，将会危及到整个使用单位的计算机网络使用安全，甚至会发生企业网络瘫痪的现象，会使得使用单位蒙受不小的损失。而对于防火墙技术来讲，虽然能够对一些病毒入侵展开防范，但是病毒形式的层出不穷，无法全面展开防护。因此，对于防火墙技术来讲，必须要对病毒库展开定期更新，从而将病毒的检测能力、防范能力提升。定时对病毒库展开更新，属于防火墙技术当中更高级别的实践应用。采取此种方式，能够更大程度的将计算机网络病毒侵犯问题做出防范，将数据、信息安全的大力维护得以实现。

2.在访问策略中的运用

防火墙技术在计算机网络安全中的运用，首先可用于访问策略方面。在访问策略中的运用，防火墙技术是通过配置的方式实现防护目的的，即通过运用相对严谨、科学合理的计划完成对计算机网络系统运行各个环节地统计、分析工作，从而更全面有效地掌握时机计算机网络的安全漏洞及防护需求，在此基础上形成相对完善、相对科学的安全防护体系，达到从访问策略层面入手提高网络安全的目的。将其运用于访问策略的过程中，主要操作流程如下：一是通过凭借单位的形式实现对计算

机网络中的数据进行划分，根据数据的不同形式以内外两种不同的访问保护进行规划，达到提高整个系统访问安全性的目的；二是结合防火墙技术的访问策略掌握用户的数据使用特点，以此为基础进行网络数据的针对性保障，确保用户使用过程中的网络安全；三是访问策略结合计算机网络的安全需求，完成对防火墙技术的优化，为计算机网络提供更有针对性的安全保障服务。

3.防火墙系统技术指标分析

学校在设置防火墙系统的时候，要对防火墙系统中一些基本功能、安全策略以及后期维护费用等进行详细的分析，这样才可以满足于学校校园网的需求。根据校园信息网的安全需求情况，在进行计算机网络防火墙应用的过程中需要按照以下几点要求来实施：①防火墙系统便于管理；在选择防火墙系统的时候需要选择那些比较容易被接受和管理的防火墙系统；②防火墙自身的安全性特点；防火墙选择时需要选择所有支持的方式，支持方式范围比较广泛，和网内认证措施之间有着比较好的衔接性和关联性，这样可以有效提高防火墙系统的安全性；③防火墙系统的稳定性；很多厂家生产的防火墙系统在还没有进行全面检测的时候就被推上市场，所以无法保障其稳定性，而在选择防火墙的时候需要选择那些经过专业网站测评合格的防火墙系统。

4.在数据信息加密中的运用

将防火墙技术运用于计算机网络安全防护过程中，能够实现对数据信息的加密保护，通过对数据信息进行加密的方式提高网络信息安全性。在网络数据的传输、存储等多个环节中，通过防火墙技术的加密功能能够避免数据在传输等过程中被窃取，是有效避免重要数据泄露、丢失的重要方式。同时，经过加密后的数据信息，能够在真实的数据外设置错误信息，达到迷惑黑客或病毒攻击的目的，能够进一步保障原始数据的完整性与安全性，进一步提高网络数据在各个环节中的安全性。防火墙技术在数据信息加密中的运用，是通过密码算法计算实现加密的，且加密形式多样化，可根据实际需求合理选择对称加密或不对称加密。

5.计算机深层检测应用

防火墙技术是目前最有效的计算机安全保护措施，可以有效改善计算机网络环境，并提高整体的安全质量，尤其经过多年的研究实践，防火墙技术在安全防护工作中的优势愈发明显。其次防火墙技术也在不断创新，可以应对更多的网络安全问题，包括深层的检测能力等，对于计算机网络的应用十分重要，针对网络内部环境进行优化和维护，有效降低网络安全隐患与风险。深层检测功能可以针对网络信息，展开全面分析、检测，并进行实时的数据追踪，确保计算机网络在运行过程中，可以受到更加直接、安全的防护。

**五、结束语**

在计算机网络技术持续发展的时代，网络作为扎根于现代社会生产各个领域的一部分，其运用安全性的保障至关重要，必须加强对防火墙等技术手段的运用，以提高网络安全性，保障用户信息数据的安全。因此，相关研究工作者应结合新时期网络技术的发展与运用特征，加强对防火墙技术等多种安全保障技术的研究运用，提高防火墙技术安全保障能力的作用，更有力地保障用户网络安全。

**参考文献：**

[1]刘曈，康红钰，刘喜民.防火墙技术在计算机网络安全中的应用[J].数码设计（下），2020，9（6）：14.

[2]赵久权.防火墙技术在计算机网络安全中的应用对策[J].通讯世界，2020，27（1）：177-178.

[3]王艳.防火墙技术在计算机网络安全中的应用探究[J].通讯世界，2020，27（2）：46-47.