 DOI: https://doi.org/10.26549/bdai.v4i3.13876

# Network Prevention Technology Based on Computer Firewall Security Barrier

**Yanxin Liu**

Jilin Jitong Information Technology Co., Ltd., Changchun, Jilin, 130000, China

**Abstract**

With the rapid development and popularization of the Internet, network security issues are becoming increasingly prominent. As an important network security device, computer firewalls can control and monitor network data, playing a barrier role. Its security and effectiveness are crucial for protecting the stability of data and network environments. This paper will discuss the basic principles, classifications, and applications of computer firewall technology in network security, aiming to provide readers with a comprehensive understanding of computer firewall.

**Keywords**

computer; firewall; safety barriers; network prevention technology

# 基于计算机防火墙安全屏障的网络防范技术

刘炎鑫

吉林省吉通信息技术有限公司，中国·吉林 长春 130000

**摘　要**

随着互联网的快速发展和普及，网络安全问题日益突出。计算机防火墙作为一种重要的网络安全设备，能够对网络数据进行控制和监测，起到了屏障的作用。其安全性和有效性对于保护数据和网络环境的稳定性至关重要。论文将从计算机防火墙技术的基本原理、分类以及在网络安全中的应用等方面展开讨论，旨在为读者提供一个全面了解计算机防火墙的视角。

**关键词**

计算机；防火墙；安全屏障；网络防范技术

## 1 引言

在科学进步快速发展的背景之下，计算机在群众的日常生活中应用也逐渐普遍，在给人们带来便利的同时也会存在一定的困扰。计算机防火墙技术作为一项安全技术能够为计算机系统的运行建立屏障。

## 2 计算机防火墙安全屏障的依据

随着计算机网络的广泛应用和数据交换的增多，网络攻击也日益增多并且形式多样化。攻击者可以利用各种手段来攻击计算机系统。首先，读取计算机数据进行攻击是一种常见的攻击方式。攻击者可以通过各种手段获取计算机系统中的敏感数据，如个人隐私信息、商业机密等，然后利用这些信息进行其他的恶意行为，如进行身份盗窃、进行网络诈骗等。其次，网站欺骗也是一种常见的攻击方式。攻击者可以通过伪造网站或者篡改合法网站的内容来欺骗用户，并获取用户的个人信息或者进行其他的恶意行为。这种攻击方式对用户的信任度和信息安全构成了严重威胁。另外，重定向攻击是一种常见而危险的攻击方式。攻击者可以通过篡改网络通信中的重定向信息来将用户引导到恶意网站，从而造成用户信息泄露或者遭受其他恶意行为。这种攻击方式往往需要利用网络路由器或 DNS 服务器等中间设备来实施。最后，操作防火墙攻击也是一种常见的攻击方式。防火墙是计算机网络中重要的安全设备，用于保护网络免受外部攻击。攻击者可以通过利用防火墙的漏洞或者不当配置来绕过防火墙，获取网络配置信息或者直接攻击其他系统。因此，保护好防火墙的安全性对于整个网络的安全至关重要。

## 3 计算机网络安全指标分析

计算机网络安全指标是评估网络安全状况的重要依据，通过对安全指标的定量分析和监测，可以帮助组织和企业及时发现网络安全风险，采取相应的防护措施。

首先，网络可用性是评估网络安全的重要指标之一。网络可用性指的是网络系统能够提供服务的可靠性和稳定

【作者简介】刘炎鑫（1984–），男，中国吉林白山人，本科，工程师，从事高速公路收费软件维护、网络维护等研究。

性。例如，网络是否经常出现故障或中断，是否能够防范分布式拒绝服务（DDoS）攻击等。如果网络不稳定或易受攻击，将对组织的业务连续性和效率产生严重影响。因此，网络可用性的指标应包括设备的故障率、恢复时间、网络中断次数等。

其次，网络保密性和完整性是网络安全的核心指标。网络保密性指的是确保网络通信过程中的数据只能被授权用户访问，而未授权用户无法获得敏感信息。网络完整性则是确保数据在传输和存储过程中不被篡改、丢失或损坏。常见的网络保密性和完整性指标包括数据加密强度、入侵检测和防御能力、身份验证和访问控制等。

另外，网络审计能力也是一项重要的网络安全指标。网络审计指的是对网络中的信息流和数据传输进行监测和记录，以便及时发现异常行为和安全漏洞。通过对网络审计数据的分析，可以帮助组织识别潜在的风险和威胁，并采取相应的安全措施。网络审计的指标包括日志记录的完整性、可追溯性、异常行为检测和报告等。

最后，网络安全培训和意识是评估网络安全状况的关键指标之一。网络安全培训可以提高员工对网络安全的认识和意识，使其具备识别和应对网络威胁的能力。网络安全培训和意识的指标包括网络安全培训的覆盖率、培训内容的有效性、员工的网络安全知识水平等。

计算机网络安全指标是评估网络安全状况的重要依据。这些指标涵盖了网络可用性、保密性和完整性、网络审计能力以及网络安全培训和意识等方面。通过定量分析和监测这些指标，可以帮助组织及时发现网络安全风险，并采取相应的防护措施。在网络安全领域，不断提升指标的水平和质量，是保障网络安全的重要手段。

## 4 计算机防火墙技术的定义和类别分析

### 4.1 计算机防火墙技术的定义

计算机防火墙（Firewall）是指用于保护计算机网络免受未经授权访问和网络攻击的技术手段。防火墙位于网络边界，通过监控和控制进出网络的数据流量，对流量进行过滤和筛选，以实现网络安全的目标 [1]。防火墙通过规则和策略来限制和控制网络中不同主机之间的通信。它可以根据源 IP 地址、目标 IP 地址、源端口号、目标端口号、协议类型等信息对数据包进行过滤和阻断。这样可以阻止未经授权的外部访问，同时也可以限制内部网络的通信流量。网络地址转换是防火墙技术中一项重要功能。通过将内部网络的私有 IP 地址转换为公共 IP 地址，使得内部网络对外部网络是不可见的，可以提高内部网络的安全性。NAT 技术还可以帮助解决 IP 地址不足的问题。传统的防火墙主要对网络层和传输层的数据包进行过滤，而应用层过滤则对网络应用层的数据进行深度检查，以识别和阻止网络应用层中的恶意行为和攻击。例如，防火墙可以对 HTTP、FTP、SMTP 等协议进行检查，以防止 Web 应用漏洞、恶意文件传输和垃圾邮件攻击等。许多防火墙产品还提供 VPN 功能，可以在公共网络上建立加密的虚拟专用网络。通过使用 VPN，可以实现远程访问和远程办公，同时还能保护数据的机密性和完整性。防火墙通常会记录和存储流经它的网络数据包的相关信息，包括来源、目标、协议、端口等。这些日志可以用于网络故障排除、入侵检测和安全审计等。审计和分析这些日志数据能够帮助识别潜在的风险和漏洞，并采取相应的安全措施 [2]。随着网络攻击手段的不断演变，许多防火墙产品还集成了智能威胁检测技术，可以检测和识别各种网络攻击和恶意行为。这些智能威胁检测技术包括入侵检测系统（IDS）、入侵防御系统（IPS）等，能够实时监测和阻断网络入侵行为，提高网络安全性。

### 4.2 计算机防火墙技术的类别

包过滤类防火墙和代理类防火墙是两种常见的防火墙技术，它们在网络安全防护方面有不同的功能和特点。下面将详细介绍这两种防火墙的工作原理、特点和应用场景。

包过滤类防火墙是最基础的网络防范技术，它通过对网络数据传递过程中的数据包进行筛选和过滤，来实现网络的安全性。包过滤类防火墙基于事先设定的规则和策略，对传入和传出的网络数据包进行检查和过滤 [3]。这些规则根据源 IP 地址、目标 IP 地址、源端口号、目标端口号、协议类型等信息进行匹配和判断，决定是否允许通过。包过滤类防火墙具有简单、快速和高效的特点，可以基于源和目标地址、端口和协议等简单的规则进行数据包过滤，适用于对网络流量进行基本的控制和筛选。包过滤类防火墙的工作速度快，几乎没有延迟，适用于对实时通信和交互性要求较高的网络环境。由于其简洁的工作原理，包过滤类防火墙可以部署在大规模网络环境中，如企业的网络边界或互联网边缘。

代理类防火墙是一种高级的防火墙技术，通过代理服务器将客户端和服务器隔离开来，在客户端和服务器之间进行中转和管理，从而实现对计算机系统的更全面的防护。代理类防火墙工作在应用层，它在客户端和服务器之间建立连接，并代表客户端和服务器进行通信。代理服务器对传入和传出的数据进行深度检查和过滤，可以识别和阻止不安全的数据和恶意行为 [4]。代理类防火墙具有更强大的功能和筛选能力，可以对传输的数据进行深度检查、过滤和修改。例如，可以检查传输的文件是否包含病毒、监控和限制 Web 应用的行为等。代理类防火墙将客户端和服务器隔离开来，使得计算机系统对外部的访问和攻击不可见，提供更可靠和安全的防护 [5]。代理类防火墙常用于企业、政府和专业网络环境中，如金融、医疗、军事等领域，用于对敏感信息和关键系统的保护。

## 5 网络防范技术的具体应用措施

### 5.1 硬件防火墙

硬件防火墙是一种实体设备，可以直观地看到和操作，便于管理和维护。同时，它们可以通过插拔来实现快速安装和卸载，方便替换和升级。硬件防火墙内部搭载有专用的防火墙软件，经过优化和定制，具备强大的安全防护能力。因此，硬件防火墙能够提供更可靠和高效的防护，比传统软件防火墙更加稳定和安全。硬件防火墙采用专用的硬件设计和优化算法，具备出色的性能和处理能力，可以支持高速网络流量和大规模用户的同时工作。此外，硬件防火墙的操作系统较为简化，减少了系统的故障风险，提升了稳定性和可靠性。硬件防火墙通常提供友好的图形界面和易用的管理平台，管理员可以通过简单的配置完成对防火墙的设置和管理。这样可以降低操作门槛，提高管理效率，减少配置错误和人为失误造成的安全风险 [6]。

CLSCO 系统是国内常见的硬件防火墙解决方案之一，CLSCO 系统内置了先进的木马、病毒和黑客防护系统，能够及时发现和拦截各种恶意攻击和入侵行为，保护企业的网络和数据安全。CLSCO 系统能够实时检测和防护文件的传输和收取过程，识别并隔离潜在的病毒和恶意文件，防止恶意软件通过文件传输途径侵入网络。CLSCO 系统可以根据企业的具体需求进行定制，从而满足不同企业的防护需求。同时，它还具备良好的可扩展性，可随着企业网络的发展而扩展和升级，提供持续而可靠的防护。由于其强大的防护功能和优良的性能，CLSCO 系统已被广泛应用于国内各大企业和机构，包括金融、电信、制造等行业，为企业的计算机网络安全提供了可靠的防护。总结起来，硬件防火墙是一种在硬件设备上运行的防火墙解决方案，具有可见、可装、可卸的特点，管理方便。其中，CLSCO 系统作为国内常见的硬件防火墙解决方案，提供了高效的木马、病毒和黑客防护，能够实时防护文件传输和收取，被广泛应用于国内各大企业，为企业的计算机网络安全提供了极佳的防护效果 [7]。

### 5.2 软件防火墙

软件防火墙是一种利用软件来对计算机网络进行防护的网络防范技术。它通过拦截、监控和过滤进出计算机网络的数据流量，以防止恶意攻击、病毒感染和非法访问等网络安全威胁。软件防火墙的主要功能包括：网络包过滤、应用层网关、虚拟专用网（VPN）支持、网络地址转换（NAT）以及远程访问等。相比于硬件防火墙，软件防火墙的性能较差，占据大量计算机内存，可能会影响计算机的整体性能。软件防火墙一般适用于个人用户，而不适用于大范围的网络安全防护。这是因为软件防火墙的安装简易、使用简单等特点，使得个人用户更容易接触和使用。例如，许多人使用的 360 安全卫士防火墙和杀毒软件就是软件防火墙的代表。它们具有安装方便、界面友好、功能齐全等优点，因此得到了广泛的用户使用。然而，软件防火墙也存在一些问题和局限性。首先，由于软件防火墙是运行在操作系统上的软件程序，因此其安全性和稳定性容易受到操作系统漏洞和攻击的影响。其次，软件防火墙的性能较差，无法满足大规模网络环境下的高并发和大流量的需求。此外，软件防火墙无法保护物理网络，只能保护安装有软件防火墙的计算机。因此，在大规模网络环境中，更倾向于使用硬件防火墙。硬件防火墙通常具有较高的性能，能够处理更多的网络流量，并可以集中管理多台计算机的安全策略。然而，硬件防火墙的安装和配置比较复杂，需要专业知识和技能，因此更多应用于企业和大型组织。

## 6 结语

计算机防火墙作为网络安全的重要组成部分，具有非常重要的作用。论文围绕基于计算机防火墙安全屏障的网络防范技术进行了深入探讨，由于技术的不断发展和网络环境的复杂性，计算机防火墙也面临着一些挑战和困难。未来，我们需要不断提升计算机防火墙的安全性和效果，以应对日益增长的网络威胁和攻击。同时，进一步的研究和创新将助力于网络防范技术的进一步发展和应用。

## 参考文献

[1] 郑秀毅.大数据背景下的计算机网络信息安全问题及防护措施[J].网络安全技术与应用,2022(8):161-162.

[2] 王晓光.计算机防火墙安全屏障与网络防范关键技术初探[J].数字技术与应用,2020,38(5):189+236.

[3] 葛小虎.关于计算机网络安全防范中防火墙技术的应用分析[J].网络安全技术与应用,2019(11):21-23.

[4] 何松.新时期下谈计算机网络信息安全及防火墙技术[J].低碳世界,2019,9(7):366-367.

[5] 冯力超.基于计算机防火墙安全屏障的网络防范技术[J].信息与电脑(理论版),2018(13):192-193.

[6] 张大鹏.基于计算机防火墙安全屏障的网络防范技术分析[J].信息通信,2018(5):166-167.

[7] 程昊.计算机防火墙安全屏障与网络防范关键技术初探[J].科技资讯,2018,16(7):90-91.