 DOI: https://doi.org/10.12349/iser.v4i3.1524

Computer Network Information Security and Its Application of Firewall Technology

Ruili Gui

Henan Economic Management School, Nanyang, Henan, 473000, China

Abstract

With the wide application of computer network and the rapid development of information technology, the problem of network security is becoming increasingly prominent. Protecting information security in computer network becomes a vital task. As an important part of network security, firewall technology has a wide range of applications. This paper will discuss the computer network information security and the application of firewall technology in it. As a security barrier, the firewall can control network traffic, prevent malicious attacks, restrict unauthorized access, and provide access control and security audit functions. By analyzing the basic knowledge of computer network, the types of network attack, the principle and function of firewall technology, we can better understand the importance of computer network information security and the specific application of firewall technology in protecting network security.

Keywords

computer; network information security; firewall technology; apply

计算机网络信息安全及其防火墙技术应用

归瑞利

河南省经济管理学校，中国 · 河南 南阳 473000

摘　要

随着计算机网络的广泛应用和信息技术的快速发展，网络安全问题日益突出。保护计算机网络中的信息安全成为一个至关重要的任务。而防火墙技术作为网络安全的重要组成部分，具有广泛的应用。论文将探讨计算机网络信息安全以及防火墙技术在其中的应用。防火墙作为一道安全屏障，可以控制网络流量、阻止恶意攻击、限制非授权访问，并提供访问控制、安全审计等功能。通过对计算机网络基础知识、网络攻击类型、防火墙技术的原理和功能进行分析，更好地理解计算机网络信息安全的重要性以及防火墙技术在保护网络安全中的具体应用。

关键词

计算机；网络信息安全；防火墙技术；应用

1 引言

随着计算机网络的快速发展和普及，信息安全已经成为当今社会中不可忽视的重要议题之一。计算机网络信息安全涉及保护数据、系统和网络免受未授权访问、损坏和篡改的威胁，以确保网络的可靠性和机密性。通过深入研究计算机网络信息安全及其防火墙技术的应用，更好地理解网络安全的挑战和解决方案。

2 信息安全的重要性

在当今数字化时代，信息安全已经成为个人、组织和社会的重要关切。随着计算机网络的普及和信息技术的迅猛发展，个人和机密信息越来越容易受到威胁。信息安全的重要性体现在多个层面，包括个人隐私保护、商业机密保护、国家安全等 [1]。

首先，信息安全对于个人来说至关重要。个人信息如姓名、地址、社交媒体账号、银行账户等，都存储在各种数字平台上。这些信息可能会被黑客、网络犯罪分子或身份盗窃者利用，导致身份盗窃、金融损失甚至个人声誉受损。因此，个人需要采取安全措施，如强化密码使用、定期更改密码、谨慎对待电子邮件附件和链接等，以保护个人信息的机密性和完整性。

其次，信息安全对于商业和组织来说至关重要。商业机密、客户数据、研发成果等是企业的核心资产。泄露或丢失这些重要信息可能导致财务损失、竞争优势减弱甚至企业破产。因此，企业需要采取有效的信息安全措施，如数据加密、访问控制、网络监控等，以确保商业机密和客户数据的保密性和完整性。

【作者简介】归瑞利（1979–），男，中国河南南阳人，本科，讲师，从事计算机研究。

此外，信息安全对于国家安全具有重要意义。在现代社会，国家安全依赖于计算机系统和网络的安全运行。政府机构、军事部门、关键基础设施等都面临着来自黑客、网络间谍和网络恐怖主义的威胁。攻击者可能试图破坏国家的通信系统、窃取军事机密或对关键基础设施进行破坏。因此，国家需要建立健全的信息安全体系，包括网络防御、网络监控、网络安全法律法规等，以确保国家安全的可靠性和稳定性 [2]。

信息安全的重要性不仅仅是保护个人、组织和国家利益，还涉及到整个社会的稳定和可持续发展。信息安全的破坏可能导致社会恐慌、经济损失和社会不稳定。例如，金融机构的信息泄露或网络攻击可能引发金融市场的恐慌和崩溃，影响整个经济体系的运行。此外，信息安全的破坏还可能导致社会秩序的混乱，例如网络犯罪的增加、社交媒体上的虚假信息传播和网络欺诈行为的激增。因此，信息安全不仅仅是个人和组织的问题，也是社会整体稳定和可持续发展的基础。

3 计算机网络基础知识

网络拓扑结构指的是计算机网络中节点和连接方式的布局。常见的网络拓扑结构有：星形拓扑（所有计算机连接到一个中心节点）、总线型拓扑（所有计算机通过一个共享的传输介质连接在一起）、环型拓扑（计算机通过一个封闭的环路连接在一起）、网状拓扑（每个计算机都与其他计算机直接连接，形成一个网状结构）。不同的拓扑结构适用于不同的应用场景，选择适合的拓扑结构可以提高网络的性能和可靠性。

同时计算机网络通信依赖于一组规范和协议，以确保数据能够在网络中正确的传输和接收。常见的通信协议有：TCP/IP 协议是互联网上数据传输的基础协议，包括 IP 和 TCP、HTTP（用于在 Web 浏览器和服务器之间传输超文本数据）、FTP（用于在客户端和服务器之间传输文件）、SMTP（用于电子邮件的发送）、DNS（用于将域名解析为 IP 地址）。这些协议定义了数据传输的格式、规则和过程，确保不同计算机之间的通信能够顺利进行 [3]。

计算机网络依赖于各种网络设备来实现数据的传输和路由。常见的网络设备包括：路由器（用于连接不同网络并在它们之间转发数据包）、交换机（用于在局域网中连接多台计算机，并根据 MAC 地址转发数据）、集线器（将多台计算机连接在一起形成局域网，但不具备数据转发功能）、网络接口卡（将计算机与网络连接起来的硬件设备）、网络缆线（用于在计算机和网络设备之间传输数据的电缆，如以太网和光纤），这些网络设备协同工作，实现了数据在网络中的传输和路由，确保数据能够准确地到达目标设备。

4 网络攻击类型

随着计算机网络的快速发展和广泛应用，网络安全问题日益突出。网络攻击是指针对计算机网络系统和数据的恶意行为，其目的可以是窃取敏感信息、破坏网络功能、获得非法利益或者干扰正常业务运作。

木马攻击：木马是一种看似正常但实际上具有恶意功能的软件。它通常伪装成合法程序，一旦被用户执行，就会在后台执行恶意操作，如窃取个人信息、远程控制计算机等。

拒绝服务攻击：DoS 攻击旨在通过超载目标系统或网络资源，使其无法正常提供服务。攻击者通过发送大量的请求，消耗系统资源或使其崩溃，从而使合法用户无法访问或使用该系统 [4]。

分布式拒绝服务攻击：DDoS 攻击是 DoS 攻击的升级版，它利用大量的分布式计算机或设备发起攻击，以更强大的攻击力量淹没目标系统。这种攻击形式更具破坏性和难以防范。

网络钓鱼攻击：网络钓鱼是一种通过伪造合法网站或电子邮件来欺骗用户提供个人敏感信息的攻击方式。攻击者通常冒充银行、社交媒体或其他信任的实体，诱使用户泄露账号密码、信用卡信息等。

勒索软件攻击：勒索软件是一种恶意软件，通过加密用户数据或封锁计算机系统来勒索受害者。攻击者要求受害者支付赎金才能解密数据或解除封锁，给个人和组织带来严重的数据和经济损失。

社交工程攻击：社交工程是利用心理学和欺骗手段，通过与人互动来获取敏感信息或获得非法访问权限。攻击者可能冒充员工、客服人员或其他可信任的人，诱使目标提供机密信息。

5 防火墙技术的原理和功能

5.1 防火墙的原理

防火墙的工作原理基于一系列规则和策略，用于过滤和管理网络流量。其主要原理包括以下几个方面：

包过滤：防火墙会检查传入和传出的网络数据包，根据预设规则进行过滤。它会比较数据包的源 IP 地址、目标 IP 地址、端口号等信息，并与防火墙的策略进行匹配。如果数据包符合规则，防火墙允许通过；否则，防火墙会阻止或拒绝该数据包。

状态检测：防火墙能够追踪网络连接的状态。通过监测网络连接的建立、终止和状态变化，防火墙可以判断是否有异常活动，并及时采取相应的防御措施。例如，它可以检测到恶意扫描、端口扫描或连接的异常行为。

地址转换：防火墙可以执行网络地址转换功能，将内部私有 IP 地址转换为公共 IP 地址，以增加网络的安全性和隐私保护。这可以隐藏内部网络结构，防止直接访问内部资源 [5]。

虚拟专用网络：防火墙可以支持 VPN 功能，通过加密和隧道技术建立安全的远程连接。它允许用户在不安全的

公共网络上建立加密的私密通信，确保数据的机密性和完整性。

5.2 防火墙的功能

防火墙作为网络安全的第一道防线，具有多种功能，旨在保护网络免受各种威胁和攻击：

访问控制：防火墙可以根据事先定义的规则和策略，对网络流量进行控制和管理。它可以允许或阻止特定的 IP 地址、端口、协议或应用程序访问网络资源，以防止未经授权的访问。

网络地址转换：防火墙可以执行网络地址转换（NAT）功能，将内部私有 IP 地址转换为公共 IP 地址，以增加网络的安全性和隐私保护。这可以隐藏内部网络结构，防止直接访问内部资源。

带宽管理：防火墙可以对网络流量进行带宽管理，确保网络资源的合理分配和优化利用。它可以根据预设策略对流量进行调整和限制，以防止某些应用程序或用户占用过多的带宽资源，影响网络性能。

内容过滤：防火墙可以进行内容过滤，检测和阻止包含恶意代码、垃圾邮件、违禁内容或非法访问的数据包。通过使用各种技术，如基于签名的检测、黑白名单过滤、URL 过滤等，防火墙可以提供对不良内容的防护。

6 计算机网络信息安全中对防火墙技术的具体应用

6.1 保护网络边界和入侵防御

防火墙的首要任务是保护网络的边界，即外部网络与内部网络之间的连接点。它可以通过配置规则和策略来控制进出网络的流量。防火墙可以监测传入和传出的数据包，并根据预设规则进行过滤和阻止。这样可以防止未经授权的访问、恶意流量以及各种网络攻击，如端口扫描、拒绝服务攻击等。防火墙还可以通过实施入侵防御机制来检测和阻止潜在的网络入侵行为。它可以识别和拦截具有威胁性的数据包，如具有恶意代码的数据包、异常流量模式和网络扫描行为等。通过及时响应和拦截这些入侵行为，防火墙能够提供有效的网络安全保护。

6.2 网络访问控制和权限管理

防火墙可以根据预设的规则和策略，控制特定用户、IP 地址、端口或协议的访问权限。通过细粒度的访问控制，防火墙可以限制特定用户或主机对网络资源的访问。这有助于防止未经授权的用户获取敏感数据或对系统进行非法操作。

防火墙还可以通过身份验证和用户认证机制来进一步加强访问控制。它可以与其他身份认证系统集成，如远程身份验证拨号用户服务或活动目录，以确保只有授权用户可以访问网络资源 [6]。

6.3 防止恶意软件和病毒传播

防火墙可以识别和阻止恶意软件、病毒和其他恶意代码的传播。使用基于签名的检测、行为分析和流量筛选等技术来检测潜在的威胁，并阻止它们进入网络。通过及时拦截恶意软件和病毒，防火墙可以防止它们对系统和数据的损害。防火墙可以与安全软件和防病毒引擎集成，实时监测传入和传出的数据流量，并对潜在的恶意软件进行识别和拦截。它还可以配置安全策略，例如禁止执行可疑的文件或阻止特定文件类型的传输，以进一步减少恶意软件的风险。

6.4 加密和虚拟私人网络（VPN）支持

防火墙可以提供加密和 VPN 支持，用于建立安全的远程访问连接。通过使用虚拟私人网络技术，远程用户可以通过加密隧道安全地访问内部网络资源。防火墙可以验证远程用户的身份，并加密传输的数据，确保数据的机密性和完整性。这对于远程办公、分支机构连接和移动设备访问等场景非常重要，可以保护敏感信息免受未经授权的访问和窃取。

6.5 日志记录和安全审计

防火墙具有日志记录和安全审计的能力，可以记录网络流量和安全事件的详细信息。利用记录传入和传出的数据包、连接请求、阻止的攻击尝试等，生成日志文件以供后续分析和调查。这些日志对于监测网络活动、检测潜在威胁、追踪安全事件以及支持合规性和法规要求非常重要。防火墙管理员可以定期审查日志，并采取相应的措施来加强网络安全。

7 结语

综上所述，网络安全是当今数字时代中不可忽视的重要议题。计算机网络的快速发展和广泛应用给信息安全带来了新的挑战。在这个背景下，防火墙技术作为一项关键的安全措施，为保护计算机网络的安全发挥着重要作用。通过控制网络流量、阻止恶意攻击、限制非授权访问等功能，防火墙有效地保护了网络资源和敏感信息的安全。然而，网络威胁的不断演变和攻击手段的复杂化使得防火墙技术也需要不断升级和改进。只有加强对计算机网络信息安全的关注，不断提升防火墙技术的能力和适应性，才能更好地应对日益复杂的网络威胁。

参考文献

[1] 吴挺.计算机网络信息安全和防火墙技术应用分析[J].中国新通信,2022,24(21):110-112.

[2] 关志聪,刁伟平.防火墙技术在计算机网络信息安全中的应用[J].无线互联科技,2022,19(10):22-24.

[3] 罗潇.新环境下计算机网络信息安全及其防火墙技术应用研究[J].信息与电脑(理论版),2022,34(8):215-217.

[4] 周旭.计算机网络信息安全及其防火墙技术应用研究[J].信息与电脑(理论版),2021,33(22):227-229.

[5] 夏文英.基于计算机网络信息安全中防火墙技术的应用研究[J].长江信息通信,2021,34(7):116-118.

[6] 黄建华,刘昕林,黄萍.新环境下的计算机网络信息安全及其防火墙技术[J].电子技术与软件工程,2021,(2):225-226.