

计算机网络安全技术在网络安全维护中的应用探讨

郭宇骞

中共天津市委党校 天津 300191

摘要：计算机网络安全技术在网络安全维护中发挥了不可或缺的作用。从基础防火墙技术的广泛应用，到数据加密、入侵检测等先进技术的联合运用，都是对信息安全的层层把关。而VPN技术和身份认证技术则进一步保障了远程访问和权限管理的安全。面对持续升级的网络威胁，我们需深入研究和应用这些技术，不断完善网络安全维护体系，确保数据的安全传输与存储。

关键词：计算机网络安全技术；网络安全维护；信息系统安全管理应用

引言：随着网络的普及和发展，网络安全问题愈发凸显。由于计算机网络联接形式的多样性、终端分布的不均匀性、网络的开放性和网络资源的共享性等因素，致使计算机网络容易遭受病毒、黑客、恶意软件和其它不轨行为的攻击。因此，计算机网络安全技术作为解决网络安全问题的有效手段，越来越受到广泛重视和应用。各种技术手段层出不穷，它们在保护网络和信息安全、应对各种网络威胁方面发挥着不可替代的作用。

1 计算机网络安全技术的概述

随着计算机网络技术的迅速发展和广泛应用，计算机网络安全问题变得越来越突出。为了保护计算机网络的正常运行和数据的安全，计算机网络安全技术发挥了至关重要的作用。（1）防火墙技术是网络安全领域中最基础、最重要的技术之一。它通过一系列的安全策略，对网络进行访问控制，防止未经授权的访问和数据传输。通过建立一道屏障，可以防止恶意软件、黑客等对内部网络的攻击和入侵。现代的防火墙技术还可以实现实时监控、日志记录等功能，对网络的安全性提供了保障。（2）数据加密技术是保护数据安全的重要手段。通过对数据进行加密，可以有效地防止数据被窃取或篡改。数据加密技术可以分为对称加密和公钥加密两种方式。对称加密采用相同的密钥进行加密和解密，其安全性较高，但密钥管理较为复杂。公钥加密采用不同的密钥进行加密和解密，其密钥管理相对简单，但加密和解密速度较慢。（3）入侵检测技术是一种主动的安全防护技术，它通过实时监测网络流量和系统活动，发现异常行为或入侵行为，及时发出警报并进行处理。入侵检测技术可以分为基于规则的入侵检测和基于行为的入侵检测两种方式。基于规则的入侵检测采用预设的规则进行匹配，实现快速响应。基于行为的入侵检测通过对系统行为进行学习和管理，实现更精确的入侵检测。（4）

VPN技术可以在公共网络上建立加密通道，使得数据在传输过程中能够得到保护。通过VPN技术，用户可以在公共网络上安全地访问公司内部网络资源，保证数据的传输安全性和机密性。VPN技术还可以实现远程办公、远程会议等功能，提高了网络使用的便利性和安全性^[1]。

（5）身份认证技术是网络安全领域中不可或缺的一环，它通过验证用户身份，确保用户对网络资源的访问是合法的和安全的。身份认证技术可以分为基于口令的身份认证和基于生物特征的身份认证两种方式。基于口令的身份认证采用用户名和密码进行身份验证，简单易行，但容易被猜测或破解。基于生物特征的身份认证采用用户的指纹、虹膜等生物特征进行身份验证，其安全性较高，但实现成本也较高。

2 网络安全维护的需求和挑战

随着信息技术的飞速发展，网络安全维护的需求和挑战也日益凸显。以下是当前网络安全维护的主要需求和挑战。（1）数据保护的需求。随着大数据时代的来临，数据已经成为企业的重要资产。数据的丢失或泄露可能对企业的业务和声誉造成重大影响。因此，数据保护成为了网络安全维护的首要需求。这包括对数据的加密、备份、恢复等方面的需求，以及防止数据被非法访问和篡改的需求。（2）系统稳定性的挑战。网络系统的稳定性是网络安全维护的基础。在网络攻击日益频繁的今天，如何保证网络系统的稳定性和可靠性是网络安全维护的重要挑战。这涉及到对硬件和软件的维护和管理，以及对网络设备和系统的安全配置和升级等方面的挑战。（3）防范高级持续性威胁（APT）的挑战。APT攻击是一种高度复杂的网络攻击，其目的是长期潜伏在目标网络中，并对目标进行长期、持续的攻击。防范APT攻击需要采取多种安全措施和技术手段，如入侵检测、恶意软件防范、网络监控等，同时也需要加强企业和组

织的安全意识和应急响应能力。(4) 应对网络犯罪的挑战。随着网络犯罪的日益猖獗, 网络安全维护也需要应对网络犯罪的挑战。这包括防止网络诈骗、网络钓鱼、恶意软件感染等方面的挑战。为了应对这些挑战, 需要加强对网络犯罪的研究和分析, 采取有效的技术手段和管理措施, 提高网络安全维护的效果和水平^[2]。

3 计算机网络安全技术在网络安全维护中的应用

3.1 防火墙技术的应用及其设置策略

防火墙技术作为网络安全的基础和核心, 起到了至关重要的作用。作为网络安全的"守护者", 防火墙有助于识别并过滤掉潜在的风险和威胁, 防止未经授权的访问和数据传输。在实际的防火墙应用中, 根据不同的网络环境和安全需求, 我们需要制定一系列具体的设置策略。其中, 最为常见的是对IP地址的过滤。通过对特定的IP地址设置过滤规则, 防火墙可以阻止来自这些地址的所有流量, 从而防止潜在的黑客攻击。端口过滤也是一个重要的设置, 它可以限制哪些端口的数据可以通过防火墙, 进一步提高了数据的安全性。此外, 协议过滤也是一个关键的设置。不同的网络协议可能存在不同的安全风险, 通过协议过滤, 我们可以限制或允许特定协议的数据传输, 从而减少潜在的安全风险。除了上述基础设置外, 针对特殊应用服务的访问控制也是防火墙设置的一部分。

3.2 数据加密技术在数据传输和存储中的应用和实现

数据加密技术是保护数据安全的核心手段, 它通过使用复杂的加密算法对数据进行加密处理, 使得未经授权的人员无法获取数据内容。这种技术在现代社会中的重要性日益凸显, 因为随着信息技术的发展, 数据已经成为了企业和个人的重要资产。在数据传输过程中, 数据加密技术可以有效地保护数据的安全。当数据在网络上传输时, 如果没有进行加密处理, 那么数据就可能被截获和窃取。而通过使用加密算法对数据进行加密, 即使数据被截获, 也无法被解读, 从而确保了数据在传输过程中的安全。此外, 加密技术还可以防止数据在传输过程中被篡改, 确保数据的完整性。在数据存储时, 数据加密技术同样可以发挥重要作用。许多企业和组织都会将重要的数据存储数据库或硬盘上, 如果这些数据没有进行加密处理, 那么一旦数据库或硬盘被盗, 数据就可能被窃取。而通过采用加密技术对数据进行加密, 即使数据库或硬盘被盗, 也无法直接获取到数据内容, 从而有效地防止了数据被窃取的风险。此外, 数据加密技术还可以用于保护用户的隐私。例如, 许多网站和应用程序都会收集用户的个人信息, 如姓名、地址、电话

号码等。如果这些信息没有进行加密处理, 那么一旦数据库被黑客攻击, 用户的个人信息就可能被泄露。而通过使用加密技术对这些信息进行加密, 即使数据库被攻击, 也无法获取到用户的真实信息, 从而有效地保护了用户的隐私^[3]。

3.3 入侵检测系统的设置和使用

入侵检测系统是一种先进的网络安全技术, 它能够对网络流量和系统活动进行实时监测, 以便及时发现任何异常行为或潜在的入侵行为。这种系统的主要目的是保护网络免受未经授权的访问、数据泄露和其他安全威胁。通过设置入侵检测系统, 可以有效地提高网络的安全性和稳定性, 从而确保企业和个人用户的数据和隐私得到充分保护。入侵检测系统的核心功能包括以下几个方面: (1) 实时监测: 入侵检测系统能够持续不断地监控网络流量和系统活动, 以便及时发现任何异常行为。这包括对数据包的内容进行分析, 以识别潜在的恶意活动。(2) 异常行为检测: 入侵检测系统使用各种算法和技术来识别异常行为, 这些行为可能表明存在潜在的入侵。例如, 系统可能会检测到大量的连续ping请求, 这可能是一种拒绝服务攻击的迹象。(3) 入侵行为识别: 入侵检测系统不仅可以检测到异常行为, 还可以识别出具体的入侵行为。这包括对已知的恶意软件、病毒和攻击模式进行识别^[4]。(4) 报警与响应: 当入侵检测系统发现异常行为或入侵行为时, 它会立即发出警报, 通知网络管理员采取相应的措施进行处理。这可能包括阻止恶意流量、隔离受感染的系统或通知其他安全设备进行联动。(5) 日志记录与分析: 入侵检测系统会记录所有检测到的异常行为和入侵行为, 以便进行进一步的分析和审计。这有助于网络管理员了解网络安全状况, 发现潜在的漏洞和威胁。(6) 与其他安全设备的联动: 入侵检测系统可以与防火墙、虚拟专用网络(VPN)和其他安全设备进行联动, 形成完整的网络安全防护体系。这有助于提高整体安全性, 确保网络在面临各种威胁时能够保持稳定运行。

3.4 VPN技术在远程访问中的应用和实现

VPN技术, 即虚拟专用网络技术, 为远程访问提供了一种安全、高效的方式。通过VPN, 远程用户可以在公共网络上建立加密通道, 实现对公司内部网络资源的访问。这种技术的应用, 不仅提升了网络使用的便利性, 更确保了数据传输的安全性和机密性。在VPN技术的实际应用中, 有多种实现方式。首先, 用户需要在个人设备上安装VPN客户端, 通过这个客户端连接到公司的VPN服务器。一旦连接建立, 用户就可以像在公司内

部网络一样访问相关资源。同时，所有数据都会在公共网络上通过加密通道进行传输，保证了数据的安全性。为确保VPN远程访问的安全性和可靠性，采取多种安全措施是必要的。首先，使用强密码和双因素认证可以增强身份验证的安全性。其次，定期更新和修补VPN服务器及客户端的软件，以防已知漏洞被利用。此外，对VPN连接进行定期的安全审计和监控也是必要的，以便及时发现并应对潜在的安全威胁。总之，VPN技术在远程访问中的应用和实现对于提高网络使用的便利性和安全性具有重要意义。而为了确保其安全性和可靠性，综合运用多种安全措施和技术手段是关键。

3.5 身份认证技术在权限管理中的应用和实现

身份认证技术是一种关键的安全措施，它的主要目标是验证用户的身份，确保他们有权访问网络资源。这种技术在许多领域都有广泛的应用，包括电子商务、在线银行、社交媒体等。通过使用身份认证技术，可以有效地防止未经授权的用户访问敏感信息，从而保护用户的隐私和数据安全。身份认证技术的工作原理是通过比较用户提供的凭据（如用户名和密码）与存储在系统中的凭据进行比对。如果两者匹配，系统就会确认用户的身份并允许其访问相应的资源。这种方法简单易行，但也存在一些潜在的风险，例如密码泄露、欺诈行为等。为了提高身份认证的安全性和可靠性，通常会采用多种技术和手段。首先，可以使用多因素认证（MFA），要求用户提供两种或更多种不同类型的凭据，如密码、指纹、面部识别等。这样可以大大降低被欺诈的风险，因为即使攻击者获取了用户的密码，他们也无法通过其他验证步骤。其次，可以使用加密技术来保护用户的凭据

和通信过程。通过使用强加密算法，可以确保即使数据被截获，攻击者也无法解密和利用这些信息。此外，还可以使用数字签名和证书来验证通信双方的身份，防止中间人攻击。除了技术手段外，还需要采取一系列管理措施来确保身份认证的安全性。这包括定期更新和维护系统，确保所有软件和硬件都处于最新的安全状态；对用户进行安全培训，提高他们的安全意识和防范能力；建立严格的访问控制策略，确保只有授权的用户才能访问敏感资源；以及定期审计和监控系统，以便及时发现和处理安全问题。

结束语

网络安全维护离不开计算机网络安全技术的支持。通过应用防火墙、数据加密、入侵检测等技术，我们能够提升网络的整体安全性。然而，网络安全威胁不断演变，我们必须持续关注新技术的发展，加强网络安全培训和防御策略的完善，以确保数据和隐私的安全。未来的挑战不容忽视，期待更多的专业人士深入研究并积极应对。

参考文献

- [1]宋晨炜.计算机网络安全技术在网络安全维护中的应用[J].信息与电脑,2020,31(20):210-212.
- [2]徐文超.浅析计算机网络安全技术在网络安全维护中的应用思考[J].中国新通信,2021,21(18):129.
- [3]查红泽.计算机网络安全技术在网络安全维护中的实践[J].电脑知识与技术,2021,15(29):19-20.
- [4]翟渊.防火墙技术在计算机网络安全中的应用研究[J].中国新通信,2022,21(18):129.