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

计算机网络安全中虚拟网络技术的应用探索

周韦韦
西安城市建设职业学院　陕西西安　710114

摘　要：为保护计算机网络信息系统的安全，妥善解决网络信息风险，如木马病毒、黑客入侵等，就必须要积极应用先进技术，本文以虚拟网络技术为研究对象，简要阐述虚拟网络技术概况及计算机网络安全的重要性，并从技术类型、应用层面、实际效果、有效措施四个方面，深入探究其在计算机网络安全中的应用，旨在强化计算机网络稳定性、保护用户信息安全性，以期为相关人员提供参考。
关键词：计算机；网络安全；虚拟网络技术；应用探索

Application exploration of virtual network technology in computer network security

Weiwei Zhou
Xi 'an Vocational College of Urban Construction, Xi 'an 710114, China

Abstract: To safeguard the security of computer network information systems and effectively address network information risks, such as Trojan viruses and hacker intrusions, it is crucial to actively employ advanced technologies. This article takes virtual network technology as its subject of study and provides a brief overview of virtual network technology and the significance of computer network security. It delves into its applications in computer network security from four aspects: technology types, application scope, real-world impact, and effective measures. The aim is to reinforce the stability of computer networks and protect user information security, providing valuable insights for relevant individuals.
Keywords: Computer; Network Security; Virtual Network Technology; Application Exploration

引言：

在大数据时代下，计算机网络安全问题令人堪忧，如何提高网络信息安全水平，是该行业领域发展的重要方向。通过引入虚拟网络技术，可凭借其安全性、可靠性、灵活性等技术优势，能够通过搭建虚拟专用网络，实现端对端的数据信息传送，提高了网络信息安全质量，大幅提升了计算机网络安全防护能力。

一、虚拟网络技术基本情况

虚拟网络技术主要依托于公共网络资源，搭建专用的信息传输通道，通过网络协议和服务供应商将各地网络用户远程连接起来，形成虚拟子网，可以让用户之间实现端对端的信息传输，有效提升网络信息安全水平。同时，此项技术的虚拟性体现在其是依附于公共网络的虚拟子网，所有用户均可以使用公共网络资源，并与其他用户分享信息，专业性体现于只能接入VPN用户，对于非VPN用户则不能够连接使用，充分发挥其搭建成本低、技术使用管理容易、安全性能极高、数据信息传输效率高、具有高拓展性和灵活性等应用优势。

如果按照技术应用方向分类，虚拟网络技术主要有三种形式，分别表现为：远程接入VPN是远程访问虚拟网络，可以将用户的客户端与服务器网关的网络连接；内联网VPN是内部虚拟专用网络，通过利用隧道技术将VPN内部网关连接；外联网VPN是拓展型虚拟网络，主要是将两个用户的VPN网络连接，从而实现网络资源链接和交流，达到数据共享下的协同促进效果[1]。

二、计算机网络安全的重要性

基于大数据时代，计算机网络所涉及的信息量增多，加之网络平台氛围的不断扩大，使得计算机往往会面临更加复杂的问题，如各式各样的病毒木马潜入网络环境

作者简介：周韦韦（1983.7），女，汉，陕西，讲师，本科，研究方向：网络技术。

中，给用户个体信息造成盗取、泄露等风险。针对计算机网络安全所拥有的独特特点，如隐蔽性强，用户进入互联网门槛较低，且自身身份信息的隐蔽性强，在盗取他人信息时，可以突破时间和空间壁垒，随意连接网络获取信息，违法犯罪过程十分隐蔽，不容易被当事人发现，所以就要持续维护计算机网络安全，做好相关防护性工作，定期升级网络信息系统，以此来保证计算机网络安全。

目前，我国高度重视计算机网络安全问题，除了大力引进和研发虚拟网络之外，还会聘请专业技术人员对虚拟网络技术加以调节和优化，从根本上减少虚拟网络环境中的消极因素，有助于促进广大群众健康、稳定上网，以防止用户信息被窃取和篡改，为广大用户的财产安全、个人隐私安全等提供保障。

三、虚拟网络技术在计算机网络安全中的实际应用

1.技术类型

（1）隧道技术

隧道技术是虚拟网络技术中的核心，可以提升数据传输质量及效率。其主要是依托于路由器网络使用端，完成通信协议加密及地址链接，搭建专用的数据传输隧道，可以让已封装的数据信息在不表达形式下借助公共网络进行传输，抵达目标地址后，隧道协议头被丢弃，加密信息也会解封，恢复数据原文表达，充分体现这一技术的安全性、稳定性的特点。目前，主流隧道技术可分为两类；一是二层隧道协议，如PPTP协议，建立远程访问的虚拟网络，将客户端与服务器连接；二是三层隧道协议，如IPSec协议，构建内部、拓展虚拟专用网络，其安全性更高，主要用于企业机密文件传输。

（2）加解密技术

从本质上来看，加解密技术是对隧道技术的进一步升级和优化，其延续了隧道技术中的点对点数据传输方式，并在此基础上科学处理数据封装，在协议中传输相关信息。如果在应用计算机网络信息中，尚未重视此项技术应用，不仅会让网络信息变得复杂化，还会降低数据信息的安全性，如黑客侵入计算机网络盗取个人信息、企业机密等。为此，就要合理应用加解密技术，依托计算机网络系统这一载体，采用科学的编程设定方式，为数据信息增设安全锁，以此来为数据信息提供安全稳定的传输环境，维护个人及企业信息安全，保护其合法权益不受侵犯，从根本上提升计算机网络安全水平[2]。

（3）密钥管理技术

顾名思义，此项技术应用对象为数据加解密中的密匙，通过依照相关基本要求，完成对密钥全生命周期流程的管理，有效防范密钥泄露等风险，从而保障计算机网络中的数据安全。具体管理内容如下：密钥生成，根据伪随机数生成器，产生相关密钥数据；密钥存储，将密钥保管在专用的存储器设备中，实现对密钥的安全存储；密钥分发，分发和共享不同数据的公共密钥；密钥备份与恢复，主要为了保障密钥的安全性、可用性，以防止密钥被破坏，加密数据信息无法解密；密钥销毁，对于使用完成的密钥进行销毁；密钥归档，将已经使用过的密钥数据进行归档存储，今后加密中不再使用，通过该流程管理，保障虚拟网络数据安全。

（4）身份认证技术

身份认证技术是验证用户身份和使用权限，通过登录账号、输入密码的方式确认用户，有效阻碍非法登录或访问资源的现象发生。作为一种成熟的虚拟网络技术，其在日常生活中应用十分广泛。例如，用户使用网银、微信、支付宝支付时，主要以输入密码、指纹，或短信验证码等方式确认身份，以防他人盗用财产；又如近年来的未成年人游戏防沉迷系统，是以输入身份信息，或面部识别等方式验证，有效控制未成年人游戏时长及充值。

2.应用层面

（1）网络

在将虚拟网络技术应用于网络层面中，首先要重点关注网络数据中心及交换渠道，采取全方位监管访问和申请的网络线路，不仅可以做到智能识别监管，又能够提高数据信息存储和管理中的安全性，以防止不法分子释放病毒或直接攻击，有效提高计算机网络安全管理能力。同时，也要定期更新和升级计算机网络安全数据，持续推进计算机网络技术现代化、智能化发展，通过增强系统智能识别能力，妥善应对后续应用中的计算机网络威胁，为广大用户提供高安全性的信息保存条件，充分发挥虚拟网络技术的应用效能[3]。

（2）软件

将虚拟网络技术应用于软件层面上，可通过保持适配性、调整协议，逐步提升计算机网络的安全性、稳定性。基于协调角度，虚拟网络技术可以合理调配服务器，高效管理计算机各类资源，全面强化系统数据处理能力。针对开放性的网络环境，为排除虚拟网络中的不稳定因素，也要实行个性化的虚拟网络设计，通过科学运用此项技术可以调整许多个性化网络，进一步提升计算机网络安全水平，并且也能对用户身份信息进行多重验证，如密码、指纹验证及面部识别等，最大限度上保障数据

传输过程中的安全稳定性。

（3）设备

将虚拟网络技术应用到计算机设备中，可通过网卡、网线、硬盘等设备，大幅度改善当前计算机网络安全环境。其一，网卡，主要是将计算机与服务器连接，在保证计算机网络安全基础上，完成数据包验证、构建专用链路；其二，网线，通过使用虚拟技术的物理功能，及时发现网络线路中的异常情况，并采取针对性手段加以解决处理，彻底消除故障隐患；其三，硬盘，虚拟网络技术的应用，可以及时升级硬盘设备，并配合日常管理维护，有效提高数据存储和传输效率。

（4）用户对接

通过应用虚拟网络技术，有效增强计算机网络安全性，可以让用户与用户间进行对接，达到数据信息共享目标，更好地拓展可利用的信息资源。一般情况下，主要有以下四点：一是防火墙，可以将计算机硬件与软件相连接，为计算机系统中资料文件提供安全性保障，尤其是应对网络中常见威胁时，如黑客攻击、木马病毒，均可起到良好的防御效果；二是选择发送途径，针对用户之间进行通信协作时，为了减少数据信息传输中的泄露风险，便可以选择一台计算机的具体传送路线；三是获取确认资料，在实际生活中的身份验证，其是利用软件对过程的精简，以便于用户获取身份认证，所以要采取综合性的核实资料，增强其安全性；四是选择安全客户，通过选取一个安全系数高、管理系统科学的客户端，确保所有信息资源存储、传输过程中的安全稳定，又可以提升工作效率[4]。

3.应用效果

（1）增强数据信息安全程度

在计算机网络运行中，安全稳定性是技术人员首要关注的问题，以避免出现黑客入侵、木马病毒及恶意程序等风险，所以就要科学合理使用虚拟网络技术，保障计算机网络信息安全。在此期间，技术人员可以采用虚拟网络技术，构建一个安全可靠、高效稳定的网络运行环境，能够提高客户端与服务器之间数据传输速度的同时，为广大用户提供更好的信息安全保障服务。

（2）快速完成数据信息共享

数据作为一种原始素材，可分为结构化、非结构化两种数据类型，如办公OA系统，财务系统等属于结构化，办公文档、图像等属于非结构化。通过将虚拟技术应用于数据传输中，可以实现二次打包，有效保护数据信息安全，防止其被他人盗取使用，并且也能够解决丢帧等问题，让数据传输更加完整。例如，将虚拟网络技术应用于高校教育教学资源管理中，除了可以防范教育资源丢失、不完整等问题，也能够将不同院校的教育系统连接起来，实现教育资源共享化。

（3）加强不同主体合作交流

第一，远程分支与企业总部之间。经济全球化背景下，企业规模逐步扩大，在不同区域中均有企业分支机构，其与总部联系主要以专线方式进行通信，费用高且不灵活。将虚拟网络技术应用其中，可以建立二者之间的数据信息传输渠道，保障远程分支与企业总部间信息传输的安全性，也能方便企业总部落实对远程分支机构的监督和管理，进一步提升二者之间的交流联系。

第二，远程员工与其他员工之间。针对新冠疫情背景下，部分员工居家工作，为保障企业正常运转，该部分员工便可利用虚拟网络技术，将自用计算机与企业网络相连接，可以远程访问企业信息系统的同时，促进远程员工与其他员工间的交流互动，确保数据信息传播的安全性、稳定性。

第三，企业与企业之间。通常情况下，企业合作方包括供应商、运输商、销售商等，在其信息交流之中经常会涉及许多机密性信息，为了保障信息交流的安全性，便可将虚拟网络技术应用其中，不仅可以实现线上面对面交流，节省双方会见时间，还能提升工作效率[5]。

4.应用策略

第一，增强网络安全意识。只有保证计算机技术人员具有良好防范意识，才能从根本上杜绝计算机网络安全隐患问题发生。为此，需要加强对用户网络安全知识教育的普及工作，积极学习网络安全知识，使其可以充分了解和认识网络安全的重要性，逐步养成良好的计算机应用习惯。与此同时，政府及有关部门也要加大教育宣传和引导力度，对广大计算机用户进行网络安全教育，通过利用微博、抖音等新媒体平台加以宣传，潜移默化地帮助广大群众形成良好网络安全意识。

第二，加大黑客防护力度。相比于普通计算机用户而言，黑客一般都具有较强的计算机技术，可以利用网络入侵用户客户端，窃取相关有价值、私密性的信息，对其造成巨大财产损失、个人信息泄露等问题。在大数据时代下，这一问题愈发凸显，所以有必要做好网络黑客防范措施，通过提升用户防范黑客意识，强化自身对黑客的理解，积极学习一些先进的网络安全技术，以保证自身信息安全。同时，企业及机构也要积极吸引计算机专业人才，定期更新和升级企业防火墙，提高自身网

络安全等级，以便于更好地防范黑客攻击，保障计算机网络环境安全。

第三，健全网络安全机制。一方面，需要完善网络使用管理机制，有关部门要大力强化对不良网站的监管，打击非法网站，彻底扫清网络环境中的风险网站、网址，并要制定详细的法律条例，让黑客认识自身违法行为；另一方面，需要实施安全防护机制，在企业中设立网络安全员，引进相关技术人员确保网络安全，切实提升网络安全防护效果。

四、结论

综上所述，虚拟网络技术在计算机网络安全中发挥了重要价值和作用，可以在保障数据信息传输安全的基础上，提高互动效率，强化工作质量，为重要数据信息管理提供便利条件。为此，就要持续、深入地探究虚拟网络技术，正确认识此项技术应用价值，从技术类型和应用层面展开深入分析，并通过增强网络安全意识，加大黑客防护力度，健全网络安全机制等，不断保障计算机网络安全性，确保数据信息资源的安全，切实提升工作效率。

参考文献：

[1]朱元凯，陈亮.计算机虚拟专用网络的安全技术分析[J].集成电路应用，2023，40（03）：114-115.

[2]阿迪娅·扎曼别克.计算机网络安全中虚拟网络技术的应用研究[J].中国设备工程，2022（12）：189-191.

[3]许镭.虚拟网络技术在计算机网络安全中的应用[J].网络安全技术与应用，2022（06）：33-34.

[4]巴根.浅谈计算机网络安全中虚拟网络技术的作用效果[J].科技风，2022（18）：52-54.

[5]李强.计算机网络安全应用虚拟网络技术的研究[J].软件，2022，43（12）：174-176.