

计算机网络安全中虚拟网络技术的运用及探讨

汤明星

武昌职业学院 湖北武汉 430200

摘要: 信息技术的发展带来了人们生活水平和质量的提高。随着当前计算机技术的广泛适应, 计算机网络安全问题越来越受到广大使用者的关注。虚拟网络技术在计算机网络中的应用, 能极大地提高计算机网络安全, 降低由于计算机漏洞为计算机网络带来的损失。本文主要研究了虚拟网络技术在计算机网络中的运用, 提出了计算机网络安全中虚拟网络技术的应用情况, 为相关技术的应用提供有效参考。

关键词: 计算机; 网络安全; 虚拟网络; 应用技术

The application and discussion of Virtual network technology in Computer Network Security

Mingxing Tang

Wuchang Vocational College, Wuhan City, Hubei Province, 430200

Abstract: The development of information technology has led to an improvement in people's living standards and quality of life. With the widespread adoption of current computer technology, concerns about computer network security are increasingly shared among users. The application of virtual network technology in computer networks can significantly enhance network security and reduce the losses caused by computer vulnerabilities. This paper primarily investigates the utilization of virtual network technology in computer networks and presents the application scenarios of virtual network technology in computer network security. It aims to provide effective references for the application of relevant technologies.

Keywords: computer; network security; virtual network; application technology

引言:

在当前的信息化背景下, 计算机网络技术的广泛使用对社会生产和生活的各方面都带来了极大的变革, 有效提高了人们生活和工作的质量。随着计算机网络技术的不断进步与发展, 要想进一步提升计算机网络的应用性能, 保证其稳定性, 必须重视对计算机网络安全的管理。虚拟网络技术在计算机网络安全中的应用, 能有效解决当前计算机网络中的容量、运行风险以及运行安全性等问题, 为计算机网络的安全稳定运行提供了良好的保障, 对进一步深化计算机网络技术的应用有着极其重要的意义。

一、虚拟网络技术的概述

虚拟网络技术在计算机网络安全中的应用, 能在计

算机公共网络中建立虚拟专用网络, 对远程访问的信息数据进行检测和管理。在虚拟网络的运行中, 涵盖了隧道技术。身份认证技术、密钥技术等技术手段, 能极大地提高计算机网络中不同区域网络之间的通信的私密性, 利用对相关信息技术的处理和加密等, 有效避免了大多数信息传输过程中相关信息被篡改和窃取的风险。当前的企业和政府等主体中的公共网络通常会应用虚拟网络技术建立专用于保护网络安全的虚拟服务器, 当网络中存在异地访问等情况时, 需要输入有效的安全密钥对内部网络进行访问, 有效提高了计算机网络中数据的安全性和稳定性。

二、计算机网络技术中虚拟网络技术的应用意义

1. 提高计算机网络安全

虚拟网络技术能利用对服务器与网络等的虚拟化, 提高计算机网络安全, 同时利用其他关键技术如隧道技术、身份认证技术、加密技术提高计算机网络安全系数, 避免计算机网络在运行过程中出现由于物理因素为计算

作者简介: 汤明星 (1984-02-01), 性别: 男, 民族: 汉族, 籍贯: 湖北省孝昌县, 学历: 大学本科, 职称: 讲师, 研究方向: 计算机网络技术。

机网络带来的信息数据安全问题，为计算机信息数据提供安全稳定的传输环境，提高计算机网络的可靠性^[1]。

2. 降低计算机网络的运行复杂性

当前计算机网络在各个领域与行业中的应用不断深入。同时随着社会的进步，计算机网络在行业中的应用越来越广泛，应用环境也越来越复杂。在这样的情况下，计算机网络在运行中产生的运行安全隐患等情况也随之增加，严重影响计算机网络在运行过程中的安全与稳定。利用虚拟网络技术，能在一定程度上简化计算机网络技术的系统运行流程，降低计算机网络的复杂性，对计算机网络系统的安全进一步进行升级^[2]。

3. 提高计算机网络中信息数据传输的可靠性

在计算机网络安全维护中应用虚拟网络技术，能直接在计算机所处的局域网内对相关的信息数据进行再次打包，识别并保护计算机网络中的重要信息数据，避免数据在传输和运行工程中被非法篡改或盗窃，有效提高了计算机网络中信息数据传输的安全性。此外，在计算机网络技术中应用信息数据进行传输，还能在一定程度上避免信息传输过程中出现的丢帧等问题，保证数据传输的完整性。

三、计算机网络存在的安全问题

1. 网络病毒

在计算机网络运行的过程中，一旦出现网络病毒入侵现象，极易导致数据等信息被破坏，甚至会带来计算机网络出现系统瘫痪等现象，严重影响计算机网络的正常使用。存在于计算机网络中的病毒具有潜伏性和隐蔽性，对计算机网络安全带来极大的破坏^[3]。因此计算机网络安全防护工作极其重要，如果没有行之有效的计算机网络安全防护措施，用户在使用过程中的一系列操作如随意打开小程序等，将会导致网络病毒停留在电脑中，导致计算机网络出现安全故障。

2. 木马病毒

木马病毒是网络病毒中较为常见，同时对计算机网络影响较大的病毒。木马病毒在计算机网络中的隐蔽性极强，随着近年来计算机网络技术的不断发展和进步，木马病毒对计算机网络运行环境的安全威胁越来越大。一般来讲，木马病毒可以分为控制端与被控制端两种程序，在计算机网络的运行过程中，部分非法分子通过木马病毒侵入到用户的计算机内，随后利用木马病毒对计算机网络的运行情况进行修改，甚至会破坏和盗取用户的相关数据信息。此外，计算机网络中的木马病毒与还能监控在计算机的运行过程，如果在使用过程中，用户不重视对木马病毒的防护工作，将会严重影响计算机网络的运行安全。

3. 对计算机网络进行非法访问授权

计算机网络中存在的非法访问授权主要是指在未经授权的情况下非法使用网络资源，一般来讲非法访问授权有非法用户对系统和网络进行违法操作以及合法用户在未经授权的情况下进行操作。非法授权访问对计算机网络的危害性较大，利用非法授权访问将会对计算机网络进行强制性的攻击，蓄意破坏系统的安全性和稳定性，引起系统运行瘫痪^[4]。

四、虚拟技术在计算机网络安全中的主要应用技术

1. 加密技术

加密技术是虚拟技术在计算机网络安全中应用最为普遍的技术，能在大多数情况下有效维护计算机网络安全，具有极其重要的应用意义。在实际应用过程中，虚拟网络技术具有一定的独立性，这需要用户首先要利用虚拟技术将当前的公共网络区域转化为自身的使用区域，并通过对相关计算机语言的使用，完成计算机网络中数字资源的转换。随后利用虚拟技术中的加密技术，抵挡计算机网络技术中的非法用户入侵、信息被窃取等情况，进而有效保护用户的隐私，降低计算机网络中由于相关隐私泄露导致经济出现一定程度损失的情况。

2. 密钥安全技术

应用虚拟技术维护计算机网络安全，还可以从密钥安全技术出发。一般来讲，虚拟专用网络技术中的密钥安全技术主要包括了ISKAMP技术与SKIP技术。通过对这两项技术的充分应用，进一步提高计算机网络安全性能。在实际应用中，ISKAMP技术主要应用的是公开密钥安全技术，用户在使用过程中能随时随地获得密钥，提高了相关操作的便捷性。然而在另一方面，利用ISKAMP技术也会产生一定的局限性，不能对计算机网络中的重要资料与数据进行有效保护。相比之下，SKIP技术主要应用的是Diffie法则，能极大地提高计算机网络中国的保密性，能在信息或资料传播过程中的全面高效地对计算机网络进行保护，有效提高用户的网络信息安全。

3. 隧道安全技术

隧道安全技术是计算机网络安全中的应用，能从源头上提高计算机网络安全性能。隧道安全技术以路由器以及各种硬件设施设备为技术，利用虚拟技术中的相关加密协议，在公共网络中将虚拟网络技术需保护的信息资料与数据进行上传，在上传前对相关信息进行二次加密，极大地提高计算机网络技术中的信息安全系数。在实际应用过程中，隧道安全技术主要通过信息解密和信息加密传输来实现。为了保证隧道安全技术的有效实现，需要保证虚拟网络具备路由器接入功能，并且还要配备隧道终止器、交换机、开通器等设备。在使用交换机时，必须要保证交换机在工作中保持良好的转换率，为隧道安全技术的应用提供科学的应用条件。

4. 身份验证技术

身份验证技术是计算机网络安全技术中应用功能较为普遍的技术。通过设置用户登录名以及用户登录密码,将初始的身份验证信息上传至计算机网络中,随后利用数据资料转换等方式,将计算机网络中的内部信息和初始信息等进行对比,生成准确的动态指令,提高用户资料和数据存储安全系数。在进行系统认证过程中,用户可以应用相应的VPC网络在计算机网络中搭建虚拟网络,并从中获取计算机网络运行过程中需要的信息和数据,从计算机网络的内部运行环境出发,检测并管理运行过程中产生的安全问题。除此之外,利用身份验证技术,还能实现对关联网络资源的扩展,进一步提高计算机网络的工作质量,强化其运行效率。

五、虚拟网络技术在计算机网络安全中的应用场景

1. 解决信息通路的安全问题

随着当前信息技术的发展,传统的计算机网络安全管理方式已经不适用于现代化的网络办公需求,尤其是在数据的处理和存储方面,往往会出现由于网络连接不科学等原因造成的信息安全问题。而利用虚拟网络技术中的VPN技术,能有效解决信息连接和传输等通路方面的安全问题,保证相关信息能及时、安全地进行传输。与此同时,利用VPN技术还能以专线的形式强化数据传输的安全性,极大地保护计算机网络的信息安全。最后,利用VPN技术还能构建专用的虚拟网络,有效防止相关信息在传输过程中由于外在因素的影响导致信息传输中存在被修改和泄漏等情况,极大地提高了计算机网络的应用便捷性。

2. 数据传输间的安全保护

首先,在计算机网络中充分利用虚拟技术建立高效的专用网络,能构建良好的信息技术安全管理系统,进而为局域网和局域网之间的数据传输提供安全保护,为用户建立有效的安全管理方式。除此之外,在内部局域网中合理设置虚拟专用网络,还能有效提高数据在高速传输过程中的安全性,同时结合密钥对数据进行保护,能有效提高防火墙的安全保护能力,为信息与数据传输提供良好的网络环境。最后通过在数据传输过程中建立稳定的网络系统,进一步提高数据在传输过程中的效率和安全性。

3. 提高用户对接企业的效率

在用户和企业之间的对接过程中,同样存在计算机网络的安全问题。要想实现用户和企业之间的有效对接,必须要优化计算机网络的安全性能。一般来讲,用户通过以下几个场景实现和企业对接的高效性和安全性。(1)当前用户和企业之间的交流都是以信息数据和资源等进行合作。为了保证信息在交流过程中不被泄露,避免不法分子趁机进行非法操作,必须要选择在信息传输和交

流过程中实现信息的安全性。(2)在储存相关资料时,利用虚拟网络技术在计算机中设置防火墙,并不断提高防火墙的安全系数,保证计算机网络中存储资料的安全性。(3)在验证相关信息和密码等环节中对信息进行定期的处理和更新。对计算机网络系统中存在的安全问题等进行及时发现并有效解决,进而降低用户与相关企业在对接过程中产生安全问题的概率。

4. 保证企业对接远程部门时的安全性

利用计算机网络技术可以实现企业和相关部门的远程沟通。在沟通过程中利用虚拟网络技术,能对企业 and 部门之间的沟通节奏进行整体把握,有效协调企业和相关部门之间的关系,提高沟通效率。同时利用虚拟网络技术还能保证企业和远程部门对接过程中相关数据资料的安全性。及时发现并制止数据传输过程中的被入侵现象,避免在数据产生过程中产生安全问题。最后,当前的企业大多已经实现了企业内部资源共享功能。利用虚拟网络技术,能加强企业内部联系的高效性,通过构建数据网等方式提高企业内部对数据和资源的管理,极大提高了企业内部工作效率和安全性。

六、结语

总之,计算机网络在各行各业中的应用越来越深入,有效地推动了社会经济的发展。无论是社会生产和学习,在使用计算机网络的过程中必须要重视计算机网络的安全问题,提高计算机网络的安全系数,避免由于计算机网络被入侵导致相关数据丢失等情况,严重影响用户的体验感。利用虚拟网络技术能有效保护计算机网络安全。对此,在计算机网络安全管理工作中,必须要充分利用虚拟网络技术中的应用优势,将虚拟网络应用于计算机网络中,降低计算机网络被病毒、非法手段等入侵的情况发生,维护整个网络的运行安全。在社会的生产和发展过程中,保护计算机网络的安全性对企业等用户的信息安全和资源管理工作有着极其重要的作用。对此,相关单位和个人必须要充分利用虚拟技术强化计算机网络安全,维护社会和经济发展的稳定性和安全性。

参考文献:

- [1]宋尊锋.浅析计算机网络安全中虚拟网络技术的作用[J].网络安全技术与应用,2022(09):25-27.
- [2]林世城.虚拟网络技术在计算机网络安全中的应用研究[J].信息与电脑(理论版),2022,34(05):204-206.
- [3]李瑛瑛.基于虚拟网络技术的计算机网络安全模式设计[J].信息与电脑(理论版),2021,33(13):183-185.
- [4]钟锡宝.计算机网络安全中的虚拟网络技术应用与探讨[J].数字通信世界,2021(03):202-203.