

计算机网络安全中虚拟网络技术的应用分析

金峰

云南经济管理学院

[摘要]文章首先针对虚拟网络技术进行了简单的概述,同时阐述了虚拟网络技术在应用过程中相对于一般网络技术的优势,进而分析了现阶段计算机网络安全中存在的风险因素,并探讨了在计算机网络安全中虚拟网络技术的相关应用。以期为我国计算机网络安全建设工作的有效发展提供有效的参考。

[关键词]计算机;网络安全;虚拟网络;应用优势;网络风险

前言:近年来频频发生的网络安全事故给计算机网络的发展和应用带来了很大的影响,网络安全时刻威胁着各个企业以及个人的信息安全和切身利益,甚至影响着国家的利益和社会的稳定。为此解决网络安全问题一直计算机技术发展领域的重要研究项目,虚拟网络技术的应用对于计算机网络安全提升有着很大的作用,可以有效保障网络用户的个人信息安全,因此,加强虚拟网络技术在计算机网络安全方面的应用研究十分必要。

1 虚拟网络技术的概述

计算机网络技术中虚拟网络技术是一项非常专业也是非常重要的技术,虚拟网络技术主要就是在公共数据网络中创建一个私有的个人局域网,以此来保障用户的个人数据信息的安全。通常情况下虚拟网络技术主要包含了以下几种:1. 身份验证技术。通过利用特殊的代码来进行用户身份的验证,这也是虚拟网络技术虚拟性的一大特点。2. 密钥管理技术。这项技术是用来给密钥进行加密处理,同时要将加密过的密钥在计算机网络平台上公开,一方面实现了虚拟网络技术对密钥的管理,同时也能够不影响计算机本身对密钥的管理。3. 网络隧道技术。通过网络虚拟技术进行数据的收发过程中,主要是通过数据包的形式来进行,但是这种网络隧道的形式存在不稳定的缺陷。4. 加密和解码技术。因为网络隧道技术不够稳定,在进行数据包收发过程中很容易受到外界的拦截或者破坏,导致用户个人数据信息受损,无法保障数据传输的安全性,通过使用加密和解码技术可以有效的弥补网络隧道技术这一缺陷,加强了网络隧道技术在数据传输方面的安全性和稳定性^[1]。

2 虚拟网络技术应用的优势

2.1 对设备要求低

通常情况下,一般的网络技术在进行网络安全管理时,都需要具备足够完善的配套设备来与之配合,而且为了实现对计算机网络技术的有效监控,就必须保证有足够多的传输帧数,因此就需要足够大的网络宽带,同时对于宽带的要求也非常高,由此可见,一般的网络技术在进行网络安全管理时,一方面对配套设备要求较高,另一方面较大的网络宽带也会造成一定的资源浪费。而虚拟网络技术与一般的网络技术相比,在配套设备以及网络资源等方面则具有一定的优势,因为虚拟网络技术只需要对少量的参数进行相应的改变就可以达到非常高效的网络安全管理,对于配套的设备以及网络宽带等要求并不高。

2.2 适用性强

在目前的计算机网络技术中,虚拟网络技术的发展已经相对成熟,在实际的技术应用中所需要的设备和配套设施等也相对完善,并且在虚拟网络技术投入使用中完全可以独立进行计算机网络安全控制,并不需要其他的技术加以配合,而且其稳定性、安全性对于其他网络技术也占有绝对的优势。为此无论是在电商产业的发展上,

还是在网络金融业的发展中,甚至是国家政府、军工行业的网络平台等都可以应用虚拟网络技术来进行计算机网络安全管控,也就是说虚拟网络技术在各个领域的适用性都很强。

2.3 运营成本低

在计算机网络运行的过程中时常会受到网络安全的威胁,给计算机网络运行效率造成了严重的影响,为此在计算机发展领域中,加强计算机网络安全管理的研发工作从未停止,并且被高度重视。但是一般的网络技术在网络完全管理时需要的设备以及对设备的要求都非常高,这样无疑会给网络安全管理的成本增加很大的负担。而虚拟网络技术在计算机网络安全管理中的应用主要是通过技术手段来实现对网络安全的管控,在设备和设施的要求上则不高,这样就可以大大降低网络完全管理的运营成本,这也是虚拟网络技术应用广泛的关键因素。

3 计算机网络安全风险因素

3.1 硬件配置不合理

计算机的硬件配置对于网络安全有着非常重要的影响,常见的影响网络安全的计算硬件配置问题主要有以下几个方面:1. 网卡配置不合理。一般情况下网卡的配置都是通过工作站的形式完成的,其在网络数据传输等方面的稳定性较低,会给计算机网络安全造成严重的影响。2. 一部分文件服务器配置不合理。文件服务器是计算机网络结构中的重要组成部分,其配置的合理性对于功能及稳定性都有非常严重的影响,如果配置不够合理就无法达到最佳的效果。3. 网络选型设计不合理。一部分计算机网络在选型设计上存在一定的不合理性,导致计算机网络的各项功能都无法充分发挥,甚至在网络功能的升级换代方面也会有一定的影响^[2]。

3.2 网络木马程序

在计算机网络中时常会有一些不法分子为了达到一些非法目的,会利用木马程序对用户的计算机网络进行入侵,然后通过对用户相关资料进行修改,并采用远程控制的手段对用户的相关数据信息盗取或者破坏,给用户的信息安全以及个人利益造成严重的影响。这种网络安全威胁是比较常见也是屡禁不止的,而且对于网络安全的影响非常严重,所以控制网络木马程序是计算机网络安全管理中的重要环节。

3.3 计算机病毒

在计算机网络安全管理中,计算机病毒也是最为常见的网络安全威胁之一,通常情况下计算机病毒对计算机网络进行攻击时多采用植入方式,以此来破坏计算机系统的相关数据程序,最终导致相关的执行指令出现错误,无法完成相应的信息管理。尤其是当计算机程序出现漏洞时就会给病毒的入侵打开方便之门,此时病毒入侵的程度会大大提高,给计算机网络安全造成的威胁也更加严重。同时计算机网络病毒还具备加强的隐蔽性、破坏性也非常强,同时还

具有一定的潜伏性, 因此所引发的网络安全损失巨大且不好控制。

3.4 非法授权访问

在某些企业内部, 企业员工为了能够取得企业内部的相关信息, 会采取编写相应的程序代码, 或者通过非法调试访问权限等方式进行非法授权访问, 从而获取个人想得到的数据信息, 不仅如此, 部分内部员工还可以通过这种方式如今企业的内网来获得自己所需要的操作权限, 从而实现个人对部分系统进行控制或者破坏的目的^[3]。而且如果是进行长时间的非法授权访问, 或者访问的内容过多, 就会对企业内部网络造成的破坏越大, 严重可能造成整个网络无法正常运作, 处于瘫痪状态。

4 虚拟网络技术在计算机网络安全中的运用

4.1 企业部门与合作客户之间的运用

目前各个企业的组织关系是非常复杂的, 为了能够使组织之间的信息传递以及沟通更加顺畅高效, 可以利用虚拟网络技术在各个部门之间进行串联, 这样可以将复杂而且零散甚至部分职能重叠的组织关系连成一个整体, 提高组织之间的信息、指令等的传递效率, 同时也能够加强对组织关系的管理。另外在企业内部的员工之间、各个部门之间、或者企业与合作客户之间经常需要进行相关数据的传递和共享, 再次过程当中必须要保障网络信息的安全性, 从而保障各方的利益不受损失, 因此可以运用虚拟网络技术来加强企业以及客户信息的安全性和隐蔽性, 可以有效防止部分非法授权访问对数据信息进行盗取和破坏^[4]。在进行企业和客户之间的数据共享时, 可以将相关的数据信息放在指定的文件夹中, 并利用信息防火墙对外界环境以及其他信息数据进行隔离, 与此同时可以设置专项的虚拟专用网络客服端登录服务器, 在保障共享数据信息的安全性同时, 也防止其访问非共享数据信息。

4.2 远程员工与企业之间的运用

虚拟网络技术还可以有效的保护企业远程员工与企业之间的数据传递网络安全, 这也是目前虚拟网络技术被视为企业计算机网络安全管理中最实用工具的主要原因, 虚拟网络技术可以有效的将企业每一位员工联系在一起, 并对相互之间的数据传递网络进行安全保护, 既提高了网络数据传递效率, 又保障了网络信息传递的安全。另外从技术领域来看, 虚拟网络技术在设计和应用过程中可以实际的考虑到每个企业的运作模式, 有针对性的进行相关方面的安全保护, 使其在各个企业的网络运作中都具有较强的适用性, 其具体的虚拟网络设计原理如下: 将企业总部设置为网络中心连接点, 根据企业运作对网络安全的需求设置相关的防火墙, 其目的在于区分企业内部员工和外部人员, 能够保障企业内部员工按照设定的方式顺利进入局域网获取工作所需数据信息, 同时能够有效的阻挡企业外部人员非法入侵, 这样就可以在保证网络信息安全的前提下实现企业内部最大限度的资源共享^[5]。

4.3 企业总部与分支部门间的应用

目前大部分企业随着自身的不断发展和完善, 都不同程度的拓展了部分企业分支, 这样企业的分支以及员工数量都在不断的增大, 需要进行的沟通会越来越多, 需要进行的的信息传递也会越来越庞大, 这给企业的管理工作增加了很大的难度, 因为在一个网络平台上很难做到对各个分支进行统筹管理, 这样就会给一些协调性工作带来不少麻烦, 比如一些分支部门之间以及与总部之间沟通不畅、各个分支部门的资源管理不合理等等。通过应用虚拟网络技术可以有效的解决这些问题, 例如通过虚拟网络技术创建可供企业内部专用的虚拟本地网络, 以此来对企业内部各个分支的管理工作, 不仅可以加强沟通协调的顺畅和效率, 同时对于资源分配和管理虚拟网

络技术也有很大的优势, 使企业的发展免受沟通不畅以及资源管理不合理等问题的影响。

4.4 信息和数据方面的运用

在当前互联网飞速发展, 已经呈现出网络信息大爆炸局面, 各种信息鱼龙混杂严重的影响着信息的时效性和准确性, 同样在企业的管理中信息管理一直是一项非常重要的管理内容。在信息和数据进行存储、传输等方面, 对网络安全性的要求极高, 但是一般的网络技术无法到达其要求的安全标准, 而虚拟网络技术因其本身具备的专用性, 就可以在很大程度上对病毒以及非法入侵进行阻挡, 另外也可以有效防御一些外界对计算机网络数据的恶意攻击^[6]。这样就可以有效的实现对网络数据的安全保护, 保障用户的信息安全和切身利益, 降低网络安全的风险。

4.5 虚拟网络技术在计算机网络安全中的发展前景分析

就目前的计算机网络发展情况来看, 在今后的发展过程中对于网络安全的要求势必会越来越高, 这也就意味着虚拟网络技术在计算机网络发展领域中的地位会越来越重要。目前在虚拟网络技术不断的应用于计算机网络安全建设的过程汇中, 其自身的实用性、稳定性以及安全性等方面也在不断的得到完善和提高, 虚拟网络技术已然成为当前最实用最有效的网络安全技术。再加上我国在电商产业上的发展正如火如荼, 虚拟网络技术在其发展过程中解决了很大的网络安全难题, 为其长期稳定的发展保驾护航。在今后的发展过程中可以针对当下信息的具体形式, 将虚拟网络技术与其他的网络技术进行有效结合, 创造出复合型网络安全新技术, 可以在很大程度上提升安全管理的质量和效果。与此同时也要在降低网络安全管理成本、优化网络安全管理流程等方面加强研究, 这也是虚拟网络技术当前发展的方向, 也相信虚拟网络技术随着不断的改进必将有更好的发展空间。

结束语

计算机网络技术的发展给人们的工作生活学习等各方面都带来了非常大的便利, 但是随着网络技术的发展各种网络风险层出不穷, 这些潜在的网络威胁一旦对计算机网络进行攻击和破坏, 轻则影响用户的体验感受, 重则严重损害用户的切身利益。有了虚拟网络技术的应用后, 计算机网络安全得到了很好的改善, 与此同时加强了虚拟网络技术在计算机网络领域的应用推广, 使其在充分发挥优势, 对整个网络领域的安全加强维护, 对于现阶段企业、个人以及其他社会组织的信息安全保障都具有重要的意义。因此相关的计算机技术人才还应该在虚拟网络的应用方面加强研究, 使计算机网络安全建设更加完善。

[参考文献]

- [1] 吴欣欣, 王鹏程. 计算机网络安全中虚拟网络技术的应用研究[J]. 计算机产品与流通, 2020(01):37.
- [2] 任均学. 新时期计算机网络安全中虚拟网络技术的应用探讨[J]. 信息与电脑(理论版), 2019, 31(24):200-201.
- [3] 孙泉, 姚连瑞. 基于计算机网络信息安全中虚拟专用网络技术应用研究[J]. 计算机产品与流通, 2019(10):71.
- [4] 李仁乐. 虚拟网络技术在计算机网络安全中的应用探析[J]. 湖北农机化, 2018(12):23-24.
- [5] 庞娜, 庞亚萍. 虚拟网络技术在计算机网络安全中的应用[J]. 电子技术与软件工程, 2018(22):201.
- [6] 蓝机满. 虚拟网络技术在计算机网络安全中的应用[J]. 黑龙江科学, 2017, 8(24):116-117.