

虚拟网络技术在企业计算机网络信息安全中的应用

李 竞*

河南农业职业学院, 河南 451450

摘 要: 随着信息技术的快速发展, 网络信息安全的重要性逐渐引起人们的重视。在实际应用过程中, 通过应用虚拟专用网络技术可以有效保障大中小型网络信息库的安全性, 有助于促进企业健康发展, 对提升网络数据安全性具有重要的现实意义。在局域网模式中, 通过虚拟网络技术可以将网络环境中的不同节点进行有效连接, 有效提升网络数据信息的安全性。因此, 有必要对虚拟专用网络技术展开深入研究。

关键词: 虚拟专用网络; 计算机网络; VPN技术

一、虚拟专用网络技术的概念分析

虚拟专用网络是在公共网络上建立的专属网络连接, 其自身具有临时性以及安全的特性。对整个网络安全信息而言, 在网络传输当中进行加密处理, 可以全面保障信息传输的安全性以及有效性。通过此项技术, 可以保障网络信息具有重要的作用。满足网络基础体系, 以便对其整体进行信息管理。对于储存传输而言, 均具有重要意义。在整个信息的加密、管理以及传输中, 计算机网络技术可以被广泛应用至各项区域主体中。通过虚拟专用网络技术, 其自身具有明显的应用优势。此外, 其具备良好的高效性、便捷性以及安全性。由于专用网络技术在传输过程中, 有可能会存在一定的安全隐患。因此, 需要借助虚拟专用网络技术, 对即将传输或已传输的数据进行一定的加密处理, 保障在处理后的信息外界无法通过常规的手段进行直接获取。其整体既可以保障信息的传输效率, 又可以降低传输过程中出现信息泄露的威胁。

此外, 在虚拟网络使用中, 虚拟网络亦具备灵活、多样的特征。在内网以及外网中有效应用, 并通过虚拟技术, 保障相关的使用者在各项区域只要借助互联网, 均可访问其相关的内网、外网, 完成拓展性的优势。获得大量的专用信息, 保障整个数据的传输更加高效、便捷, 达到使用标准^[1]。

二、虚拟专用网络技术的分类

(一) 加密技术

虚拟专用网络采用了专门的数据加密技术, 来保证虚拟网络中的数据安全, 通过编码将传输的数据变为乱码的形式, 使得网络中的数据能快速传输到目的地, 能够快速发现计算机网络信息系统中存在的网络安全问题, 并能采用有效的技术措施进行处理, 弥补网络通信中可能产生漏洞, 以保证通信网络的安全。采用数据加密技术可以有效对网络通信的数据进行处理, 能避免信息丢失泄露而对企业造成影响, 在虚拟专用网络中, 数据加密技术十分重要, 在具体的数据处理中, 要求相关工作人员重视, 充分地运用数据加密技术提高网络的安全性。加密技术也能够拥有隧道安全技术中, 进一步提高虚拟专用网络的数据安全。

(二) 身份认证技术

ID认证技术是重要的VPN技术。它在人们的生活中得到了广泛的应用, 在确保计算机网络的信息安全方面起着非常重要的作用。例如, 现代购物在现代人中很流行。购买商品、火车票、飞机票、巴士票等时, 必须验证真实姓名。如果使用支付宝或网上银行付款, 则还需要执行银行交易并保存用户信息。查看真实信息和真实姓名使在线购物更加轻松。银行使用多种验证方法来保护用户资产。近年来, 我国的电子商务行业发展迅速, 揭示了身份验证技术在保护计算机网络中的作用。它变得越来越受欢迎。

(三) 密钥管理技术

密钥管理技术由SKIP和ISAKMP组成, 也是确保在线安全传输用户数据的重要技术。SKIP对于虚拟网络中的信息

* 通讯作者: 李竞, 1974年12月, 男, 汉, 河南息县人, 现就职于河南农业职业学院, 副教授, 本科。研究方向: 图像处理, 网络技术, 数据库应用。

化技术,可以起到良好的保护作用。但SKIP的不足在于,其无法在网络处于正常运行状态下,做到有序传输信息数据,实现数据共享;SAKMP既能有序传播数据信息,又能提升密钥管理技术的安全性、稳定性,防止数据信息被网络黑客窃取。用户可以设置DES密钥对重要的数据信息进行二次加密。当有用户忘记密码时,借助RSA密钥可以快速恢复数据。但是,ISAKMP技术与SKIP技术是相反的,即密钥是公开的,任何人都可以使用。因此,必须实时使用密钥管理技术以防止数据泄露。

(四)隧道技术

在应用过程中,对于专用虚拟网络技术而言,利用隧道安全管理技术,可以在目前的技术体系中,按照整个数据化的特点对数据信息完成分析处理,实现安全传播的手段。保障整个数据库具有明显的安全特性,在应用隧道技术进行计算机安全管理过程中,可以完成处理整合的方法。对整个数据包进行封装处理,并在运输过程中,结合隧道技术的特性,进行优化。例如,在整个数据包中,可以额外附加相关的路由信息,以保障整个隧道技术能够对相关数据包实现有效的安全保障。

三、虚拟专用网络信息安全的应用措施

(一)应用在企业总部门与远程分支机构之间的信息安全管理

在不同的大型企业中,总部往往与各地分支机构之间存在着很大的业务交流与数据共享,需要采用有效的安全措施来保证它们之间往往需要数据共享与数据传输,采用虚拟专用网络可以保证企业的总部与各个分支之间的信息交流的安全性及有效性,才能有效提高企业信息交换的效率,才能有效保证企业的经济效率。采用虚拟专用网络,在企业的综合与各个分支机构、供应链之间搭建通信的桥梁,企业总部、各个分支机构可以通过虚拟专用网络建立虚拟局域网进行远程网络虚拟会议,在提高网络通信效率的同时,而且在这一网络会议中,还可以进行数据资料演示和传输,方便企业的各个部门、分支机构参与到会议讨论与学习中,在提高各个部门之间相互效率的同时,采用虚拟专用网络的一对一、点对点、一对多的通信加密技术,保证企业与用户之间能进行安全的贸易,还能有效避免企业的商业机密被窃取,从而为企业的安全通信提供服务^[2]。

(二)加强远程员工与公司之间的联系

在远程员工和公司之间进行通信时,可以使用公司的本地网络。这是一个虚拟专用网络技术应用程序。由于某些公司员工不在同一地点,因此该技术使远程员工可以随时轻松地与公司报告,从而改善了对公司的整体控制,例如当远程员工需要发送文档时,在工作中或需要管理层提供建议时的重要问题,VPN技术可以在整个公司范围内快速有效地部署。公司可以远程监控员工,因为他们可以很好地进行沟通。想象一下时间和动态控制。如果要使用此技术,则需要总部作为应用中心。公司Internet网关可以补充Internet防火墙设备,以允许其他用户通过VPN登录到客户端并获取必要的信息。客户可以共享资源,信息并促进员工与公司之间的沟通。

(三)提升产品的安全性以及质量

在发展过程中,如应用虚拟网络专用技术,可以保障计算机自身的安全性以及质量能够明显提升。VPN技术在使用中,外网或内网的核心节点有可能会遭受IPS以及IDS劫持攻击,导致计算机无法使用或计算机网络信息出现泄露的威胁。此外,针对VPN提供商而言,VPN提供商如无法对自身的VPN产品质量及安全性保障,将会导致其存在安全漏洞,甚至远程代码漏洞。必须加大VPN的开发以及监管,以保证整个用户之间其漏洞能够有效的修复,并对SDL进行优化。在提升安全性以及质量中,需要对整个VPN状态进行合理有效的设计开发,借助安全测试的模式,准确识别相关的记录,并对问题整体进行设置,全面提升VPN的安全性能。

此外,在必要时,针对VPN技术,可以创建应急响应模式。采取相应的措施以介绍安全事件将会对用户以及使用者所带来的不良影响,通过完善漏洞以及维护其他管理方案,可以实现企业的全面管理融合。此外,亦可以借助谷歌、微软等企业的漏洞扫描方法,以保障其具备自动化的优势。解决学校安全问题,以实现信息的全面安全管理^[3]。

(四)优化整个安全防护模式

在计算机网络安全技术中,其整体存在着明显的隐患以及风险。对相关的安全隐患进行分析,可以得知安全隐患主要来源于黑客。如在使用过程中,黑客通过特殊手段对计算机系统进行攻击,将会导致计算机系统出现运行风险。相关漏洞将会使使用者的个人隐私遭受严重威胁。在具体的改进方法中,可以结合黑客攻击的技术以及黑客攻击

后计算机出现的相关缺陷,有效地分析出黑客目前所采取的行动以及黑客在网络技术中的攻击目的。并实现合理、有效的改进方法,保障整个计算机能够实现安全管理。

此外,在监管技术中,必须要结合我国的法律法规,优化整个安全防护系统。及时搭建合理且有效的网络架构系统,并通过动态监管等特征,全面保障计算机系统能够有效运行。利用密码技术以及入侵检测技术,创建相关的安全防护体系,满足风险防控基础要求^[4]。

(五) 在技术人才队伍建设中的应用

为了提升对虚拟专用网络技术的应用效果,企业需要组建专业技术团队,引进高素质的技术型人才,定期开展专业知识教育与培训,让其可以及时掌握最新的知识技能。相关工作人员借助虚拟网络的特殊技术可以通过本地网络进行协商,有利于及时解决相关问题。

四、结束语

综上所述,在实际应用过程中,通过应用虚拟专用网络技术可以有效保障大中小型网络信息库的安全性,有助于促进企业健康发展,对提升网络数据安全性具有重要的现实意义。

参考文献:

- [1] 习毅.虚拟专用网络技术在计算机网络信息安全中的应用探讨[J].数码设计(下), 2020,9(6):96-99.
- [2] 周康乐.基于虚拟专用网络技术在计算机网络信息安全的分析[J].文渊(中学版), 2020,11(7):243-244.
- [3] 刘磊.虚拟专用网络技术在计算机网络信息安全中的应用探讨[J].信息与电脑, 2020,32(13):187-188.
- [4] 柳成霞.虚拟专用网络技术在计算机网络信息安全中的应用[J].数字通信世界, 2020,33(11):177-178.