计算机网络信息安全中防火墙技术研究

符勤祖
中海油信息科技有限公司 北京 100000

摘 要：近些年，计算机网络技术性发展迅速，为各行各业发展带来了技术保障，数据信息数据量不断增长。系统运行具备开精神性等特性，给互联网数据通信安全性导致了巨大威协。网络技术的在推进社会发展发展的前提下，也出现了许多电脑病毒，经常发生故意黑客攻击状况。为了防止这种现象产生，必须提升互联网数据通信与存放安全性。而防火墙技术可以通过防护本地连接充分发挥安全防范功效。为了能促进防火墙技术在计算机网络安全性中实现更高功效，必须贯彻落实该方法，提升计算机网络技术性发展安全性，促进社会发展不断发展与发展。

关键词：计算机；网络安全；防火墙技术；有效应用

引言

新的发展阶段，信息内容向着经济全球化的方位推动，互联网技术开始在大家生产制造和生活的各个方面得到广泛运用，也在一定程度上进一步促进了计算机网络的发展。应对信息化社会中对计算机网络各个方面不同类型的规定，计算机网络的发展速率获得了进一步的提高。也也正是因为计算机网络应用领域比较广泛，因而经常会出现一些病毒攻击、黑客入侵安全隐患，不但会对计算机机器设备造成影响，并且还会对计算机网络网络信息安全造成巨大危胁。因而，针对计算机网络信息安全隐患进行全方位的解读，积极主动选用例如防火墙技术等有效应对策略，从而为计算机网络网络信息安全给予足够的保障。

1 计算机网络安全中防火墙技术的概念分析

防火墙技术说白了，便是在计算机网络运作的过程当中，根据信息技术性构建起一堵能够阻拦火灾事故混乱的墙，避免废弃物信息和黑客攻击，合理阻拦和申请注册外界不明信息数据信息，产生病毒感染初始数据库系统，完成高效率防火墙技术主要有两种明显的功效。最先，防火墙技术能够监控和挑选计算机软件在使用中流动信息数据信息，次之能够及时出现异常的信息数据信息并传达给客户，防止了一些垃圾数据和没用数据库的存有造成系统运行不通畅和交通阻塞问题因而，根据合理应用防火墙技术能够加速计算机使用效率，防止运行时遭受外界病毒侵略，给予平安稳定的计算机网络服务项目。第二，防火墙技术能够一键备份管理方法计算机网络运作中存在的数据信息信息，防止忽然的互联网安全事故所造成的财产损失，防火墙技术的出现也会导致电子计算机内部结构信息毁坏和不正确等诸多问题

2 在计算机网络安全性中运用防火墙技术的重要性

在计算机网络安全性中，运用防火墙技术具备十分必要和重要意义，主要表现在以下几方面。一是运用防火墙技术，能够高效管理不安全的服务项目。因为计算机网络自然环境尚不稳，很容易出现安全隐患，防火墙技术的应用能够合理地管理方法不安全的计算机网络服务项目，尤其是内部结构网络信息和外部网络数据信息或者通过协议书方法确保网络数据传输安全性，防止内部结构关键网络信息被泄漏，防止内部网络和外部网络遭受黑客攻击，计算机网络安全性能；二是合理运用防火墙技术，控制能够浏览特殊网址。很多房子在浏览、传送数据的时候需要独特维护，仅有得到许可证的别的服务器才可以互换数据信息。这一高效的防护措施能够减少不必要浏览，防止违法盗取数据资料的现象。除此之外，除非是必需，不然务必限制访问以有效控制计算机网络信息。三是防火墙技术容许集中化安全防范。

与分散化摆放安全防护设备对比，这类集中化防护措施更容易揭露维护实际效果，有效控制关键信息数据信息，将身份证件立即留到正本上，将登陆密码、登陆密码表述放到网络防火墙中，开展多种安全防护。四是计算机技术防火墙技术有益于对内网和外网上流通传送数据、数据库访问进行系统记录并形成日志。日志的功效特别大，是当代可能出现的进攻的重要指标，务必充分运用日志的功效，执行有目的性的防护措施。

3 防火墙的主要类型分析

3.1 应用代理型

作为一种比较常见的防火墙技术，APP代理型防火墙技术都能够运用特定代理技术性添加另一个TCP联接以确保防火墙的正常运转。该防火墙技术的关键部分为代理服务器架构，它意味着手机客户端根据程序执行来源于云服务器联接要求，并且在内部网络接到来源于外部

网络连接服务项目申报时开展无线中继。根据代理网络服务器接受并认证来源于手机客户端连接服务项目审核后，向服务器发送有关信息。从具体关键技术情况看，该防火墙技术可以有效地检验不一样APP网络层中涉及到的数据包，并把所得的信息置入管理决策中，最大程度地确保计算机网络运转的安全性。

3.2 分组过滤型

包过虑型防火墙技术，又被称为包过虑网络防火墙，本身有好用、简易、便捷等众多特性，在接入各种各样计算机设备时，能够严禁一些TCP/IP，还可以严禁电子计算机与其它防火墙技术对比，这一类型的防火墙技术具备高效率、靠谱等特点，能够给客户一定的开放性，但是也要意识到仅有内部结构地址的数据包才可以进出。针对外部的获得的数据包，防火墙技术严禁数据包进到。在公共网络层面，该防火墙仅允许地址端口是80的数据包进入。

3.3 复合型防火墙

作为一种复合性防火墙，该防火墙技术性具备运用代理商型防火墙移动和包过滤型防火墙的优点，能够表明更加好的网络信息安全实际效果，推动计算机网络的安全运营。运用复合性防火墙时，在ASIC架构设计的影响下，根据集成化计算机网络里的信息和数据和病毒感染，过滤在其中的危险性信息内容，确保计算机网络运转的平安稳定。此外，运用复合性防火墙时，以多寄主构造为主导，开启计算机网络的安全防护实力，且支持网络端口及多LAN管理，对内部的私有网络进行有效划分，进一步提高用户的网络使用安全。

3.4 状态检测型防火墙

状态检测防火墙实际是传统式分类过滤的拓展，可以通过应用状态检测分类过滤技术性来测试和过滤通过IP地址、服务器端口和TCP标签的分类，但是该优化算法状态检测防火墙安全系数好，而特性高效率、扩展性好，运用覆盖面广，但容易造成数据延迟。

3.5 分布式防火墙

分布式防火墙是重要存在网络主机中常发放给软件系统的防护软件。分布式防火墙的分布式构造从根本上解决了传统式防火墙容积低、特性低、扩展性弱等诸多问题。分布式Crossbar体系构造彻底能够满足性能卓越和灵便拓展的需求，但分布式防火墙安全性比不上别的防火墙技术性。

4 计算机网络信息安全中防火墙技术的应用

4.1 安全配置中的有效应用

分开的电子计算机都将独立设定安全性服务隔离地区，但是该防护地区与其它网络服务器和管理信息系统设备有很大的不同。防护地区是内部网不可或缺的一部分，做为单独的局域网络，在确保服务器数据运作安全与此同时，还可以为全部管理信息系统的正常运转保驾护航。将防火墙关键技术于被动安全后，可以借助网络地址转换技术性，应用投射方法使内部网里的主机地址变成防火墙的高效IP地址，使全部主机地址处在维护情况通过各种设定方法，能够避免外部把握内部网的构造，无法获取计算机真正IP地址，进一步提高内部网安全性，尽量避免公共网络IP地址的使用时间。因而，在计算机网络安全性中，运用防火墙技术性可以有效的操纵运营成本。应用计算机网络时，经营单位能够科学合理设定界限无线路由器，使企业计算机网络具备过滤作用，与此同时依靠防火墙技术性将计算机网络与内部网有机化学相互连接。此外，界限无线路由器也可用作没有在安全性服务隔离区域内的群众网络服务器。那样，不需要此外设定防火墙，就能在界限路由器和拓扑结构的支持下保证计算机网络的安全性[5]。在这个设定下，不但可以快速地服务隔离地区互联网的安全性，并且能够确保全部计算机软件的安全性能，便捷外界客户区域范围电子计算机内部网。不难看出，防火墙技术的应用计算机网络安全性中的运用具有较高的实用价值。

4.2 访问加密

黑客入侵都是互联网信息安全性普遍危胁之一，不但危及互联网信息安全性，也会对用户导致不良影响。可是防火墙技术性可以根据计算机软件所受到的侵略状况，从互联网信息安全性角度考虑，给用户开展预警信息，最大限度确保用户安全性。防火墙技术性里最为中心的技术性便是数据加密，在互联网信息安全管家运用，发挥出自己的实用价值。不但可以有效阻拦外界风险信息进到内部网，也可以对内部结构全部信息开展数据加密，防止出现违法盗取和伪造。全部进到互联网的用户信息都能被数据加密解决而且储存，信息泄漏风险性降到最低。仅有键入正确登陆密码、账户等身份认证信息后，才能够进入应用系统，假如输错防火墙技术性还会继续弹出提示框不正确预警信息，初始登陆用户还会在第一时间接到对应的登陆警示，不法侵害、违法盗取等诸多问题都可以得到一定预防避开，互联网发案率大幅度减少。从互联网信息安全性角度考虑，不法侵害是比较常见的现象，防火墙在实践应用全过程之中建立了有针对性的防御系统，造就了井然有序自然环境，网站运营信息具体内容得到保障，并且能有效区别。防火墙从产品、互联网技术2个视角下手，展开更深层次的

整体规划、搭建，用户在前提条件下使用网络不但自己的信息获得维护，手机上网活动更安全。例如：新形势下防火墙安全防护相关工作的人性化提高，根据自己的访问个人行为对互联网开展安全防护，不断提升总体安全设置，产生相对应解决措施流程，“一针见血”发挥其重要男性性功能，让网络安全预防实际效果获得从根本上提升。简而言之，浏览加密算法便是较为常见的身份认证和加密算法，不但可以确保商业秘密信息的安全性，还能够阻拦外界进攻，最大限度限制信息病毒传播途径。

4.3 应用网关防火墙

相比于其他互联网信息安全防范方式来讲，网关防火墙拥有更为靠谱安全性，而且在长久的运用和改善下，运用网关防火墙慢慢开始朝着网络层方向发展，运用网关防火墙这样的优点是一般包过虑防火墙所无法相比的。在具体用的过程当中，用户利用计算机对输数据信息时，要进行重复认证，仅有在成功认证前提下才可以浏览互联网资源，当用户发生认证不正确的情形下往往会阻拦浏览，这在一定程度上防止了互联网信息安全风险的诞生。一般来说，运用网关防火墙的认证方式为用户名、登陆密码及其动态口令，总体认证实际操作十分简单，若网络黑客对互联网开展进攻，则DoS进攻时间很短，无法对互联网导致合理攻击。次之，运用网关防火墙一般分成两类，一种是联接网关式防火墙，另一种是直连式防火墙，联接网关防火墙有比较多的信息条文必须验证，在运用的过程当中可以借助捕获手机流量的形式进行认证，维护网络层安全性，可是直连式防火墙不具备这类作用。在实践应用的时候还必须以具体情况为基准挑选适度的防火墙方法。

4.4 日志监控中的有效应用

将防火墙关键技术到电子计算机网络信息安全日志监管中，是一种安全防护使用价值相对较高的方法。一些工作人员在收集日志信息时，大部分都会全方位收集全部有关信息。这种做法必须消耗的时长比较多，并且所收集的信息目的性较弱。互联网时代，防火墙技术性自身信息量极大，若是在互联网运行时出问题，便会外流许多关键信息。因而，为解决这一问题，必须管理者在信息收集时会着重点和目的性，关键收集这些重要信息，这样既能提升了信息收集高效率，并且还能提升信息的目的性，将信息隐性的使用价值充分运用出去。因而，将防火墙关键技术到日志监管中，能够避免收集这些使用价值信息不太高乃至无价值的信息，提升信息收集的实效性高效性，合理缓解相关人员的工作量。

4.5 协议技术

防火墙协议技术是指用户在进行外来信息下载过程中，根据预先设置每一次信息传送字节，以确保全部数据信息信息传达的容积尺寸，一旦出现掩藏病毒欠佳信息文档会超出事前设置的信息传送字节，这时候防火墙的安全防护视频监控系统就会自行终止数据信息信息的传送，以合理阻隔欠佳信息，既有利于数据信息信息的传送与接受，又可增强网络信息安全防护抗压强度，特别是数据信息信息传送违法行为的出现异常也会引起用户的警惕，这有利于提高用户的信息安全防范观念，以确保用户都可以正确对待防火墙技术的价值，并科学合理把握防火墙技术的发展基本原理，进而确保互联网信息安全性。

结束语

不难看出，防火墙科技的应用针对确保互联网信息安全性拥有很关键的功效。在信息化技术快速发展的趋势下，为充分保证互联网信息安全性，就必须得对防火墙技术实现持续不断的升级及其提升，与此同时建立相应的法律规范构建融洽的网络空间，高度重视用户对计算机网络的规范性，提高用户充沛的信息安全防范意识，全方位搭建合理安全应用系统，尽量减少木马程序及其网络黑客进入等对互联网信息安全性导致危胁，保证互联网信息安全性。

参考文献

[1]戴辉.计算机网络信息安全中防火墙技术的应用探究[J].信息与电脑(理论版),2020,32(01):227-228+231.

[2]杜博杰,钟慧茹,葛运伟.计算机网络信息安全中防火墙技术的有效运用分析[J].中国新通信,2020,22(01):154-155.

[3]陈军.计算机网络信息安全及其防火墙技术应用研究[J].中国新通信,2020,22(19):129-130.

[4]王雷.计算机网络信息安全与防火墙技术的应用[J].产业科技创新,2019,1(23):66-67.