计算机网络信息安全中防火墙技术研究

张　宁
济南市气象局　山东　济南　250000

摘　要：在计算机网络信息技术迅速发展且广泛运用的各行业里，既给人们生产活动有效化、高效化带来了服务支持，又出现了严重的网络信息安全隐患，可能会对大众的进一步权益造成威胁。因而，在新领域下，计算机网络信息安全隐患及处理成为了各界人士相对高度关注的焦点课题研究。基于此，文中主要是针对新领域下计算机网络信息安全隐患展开分析，并且从防火墙技术层面探索合理安全防范措施，致力于提升计算机网络信息安全标准，以更好的服务于我们的生活和工作。

关键词：新环境；计算机网络信息；安全；防火墙技术

引言

现阶段，网络安全性变成各界人士关注的焦点内容。对于规模性网络恶意攻击，根据提升防火墙技术，能提高网络安全性，同时还可以处理现阶段和未来网络安全隐患。在实际应用中，根据国家网络检测标准，防火墙对信息进行可选择性限定，以保证网络的正常运转。

1 相关概念解析

1.1 防火墙技术

当代防火墙技术，主要用于网络中根据网络安全视角而采取的一种多构件组成，是计算机网络安全生产技术的一个基本上构成部分，都是非常常见的计算机网络安全防范技术之一。伴随着计算机网络方式的改变和发展趋势，尤其是无线传输技术给计算机网络增添了又一次的发展机遇，并且也给计算机网络安全出了更多的考验。因而为了确保计算机网络可以顺畅、安全运作，防火墙理论是其底层安全防范最经常应用的一种安全防护技术。防火墙技术能够及时的避免恶意网络损害，还可以安全防护病毒感染损害。比如客户从网络中进行压缩文件下载，非常容易进到一些具备不可逆或是存有损害客户信息的后台设置，防火墙就能实现及时地提示、警告或阻隔浏览等行为，充分保证计算机网络安全。

1.2 计算机网络安全

计算机网络安全是一个比较广泛这个概念，可以看作是保障存在网络里的软、硬件设备在运转及管理过程中预防遭受网络上非法行为损害。计算机网络安全一般能从两方面开展掌握，一是物理学方面的计算机网络安全。物理学方面主要指避免计算机物理设备或网络物理设备因外力作用毁坏而造成网络信息的损坏遗失。二是逻辑性方面的计算机网络安全。逻辑性方面主要是针对系统运维，避免数据信息根据不合法的网络方式方法而出现损坏或损失[1]。

1.3 技术特点

（1）具备管控通信的特点。具体开展网络信息传送时，应依靠防火墙，对信息互换开展有效控制，搭建安全网络环境，把风险信息防护到通信系统之外。对于全部进入内网络的信息，一般还要依靠防火墙技术开展查验，若是运用此项技术检测出来不达到互联网技术规范标准的信息，那样将开启自我防御系统软件，把有关的信息所有彻底删除，防止不安全的信息登录系统内部结构。（2）具备安全防范的特点。根据计算机的兴起应用，促使大家的生活状态出现一定的改变，促进公司经营管理方法都进行了改善，电商等大数据技术赢得了普遍存在的应用，尽管可以为大家给予比较大的便捷，但这一过程中，又为犯罪分子创造了机遇。有些网络黑客可以通过计算机网络系统软件，进攻这其中的网络安全问题，进而获得别人的信息，进一步完成其社会经济目地，这将会对别人造成无法估量损失。根据防火墙科技的应用，能够全面实施安全防范功效，根据内外网信息开展互换时，能有效防止违法信息登录系统内部结构，从而全方位确保计算机网络安全，确保相关工作成功开展。

2 计算机发展中存在的安全问题

2.1 病毒感染以及黑客攻击

计算机网络的应用在一定程度上意味着一个企业现代化发展的水准。计算机网络因其便捷性及其专业性可以为公司带来一定的经济效益，可是同时为网络攻击造就了非法操控的标准，计算机内部结构程序及其软件会由于一些网络病毒感染导致感染，计算机系统软件也可能因为感染病毒而造成使用效率的降低，一些关键的信息就会受到威胁，严重危害计算机网络的安全性。而测算网络安全性中另一项非常危险的安全隐患便是网络黑

客攻击，隐蔽是网络黑客的主要特征，可以对计算机信息导致无形中间的毁坏或是信息盗取。计算机信息其价值会因越来越多网络数据信息而随着减少，在这样的标准下将隐藏的网络黑客寻找出来就十分困难，采用不正当手段的方法对网络开展进攻是网络黑客的常用技术手段，网络的正常运转及其计算机安全隐患也会受到网络黑客威胁[2]。

2.2 用户操作不当

计算机网络安全系数有可能会遭受人为因素操作及其网络管理人员工作不合理而受影响。针对计算机网络实际操作专业能力专业知识及其网络安全技术规范的欠缺会往往因为操作失误而造成计算机网络安全问题的诞生，可能会导致一些关键信息的遗失，或是遭受网络黑客攻击对消费者造成极大的损害。此外，计算机本就是属于机器的一种，维护保养及其维护保养针对计算机的应用是极其极为重要的。而现实生活中好多人并不重视这一点，计算机损伤以及对于计算机网络管理方法的不当，诸多安全风险的形成造成信息的遗失对消费者造成不良影响。

2.3 计算机网络系统管理漏洞

计算机网络管理信息系统同样也会对消费者信息安全产生一定威胁，目前计算机信息安全防范中依然存在着管理不到位完备的难题，不够重视对计算机网络日常维护，缺少对计算机网络信息防范意识，尤其是在一些企业客户对其计算机使用中，管理模式的不完善，可能提升计算机网络信息泄漏风险，乃至为企业的发展产生一定伤害。

3 防火墙类型分析

3.1 网络级防火墙

主要在网络层与传输层间发挥出功效，一个路由器是一个传统式网络级防火墙。此类防火墙通过分辨外部数据库的服务器IP、总体目标详细地址及其端口号，检验数据文件的各种信息能够与防火墙设定的过虑数据信息相符合，进而分辨这条数据信息能够通过外部网络传送至内部结构网络。一般情况下，网络级防火墙默认设置原则是防护墙丢掉此IP包，从而减少故意违法连接进入计算机网络系统。

3.2 代理服务防火墙

此类防火墙代表的是一个专用型网络与互联网通信连接的防火墙，关键是在网络层使出它的作用。此类种类防火墙能够提供二级连接而且变换详细地址，以此来实现内部结构网络和外界网络相互之间隔绝的功效，可以对进出防火安全的所有数据信息开展实时监控，具有一定的密钥管理、全方位记录日志及其审计的作用。此类种类防火墙的应用能够进一步提升计算机网络信息的稳定性及安全，但是这会让网络特性大幅度降低[3]。

3.3 状态检测防火墙

此种防火墙是一般包过虑防火墙特性里的扩展，其有较好的扩展特性、相对较高的应用安全系数、配备方便快捷、应用领域普遍等优点，主要是在网络层、网络层和传输层中充分发挥。此种防火墙具备检验模块捕获数据文件，可以对数据文件IP地址、端口号及其TCP标识开展过虑，与此同时凭着对应的优化算法分辨进出网络层的信息数据信息，能让手机客户端和服务器搭建更为直接的相关性，还能够对UDP协议书开展比较有限的大力支持，从而实现对每层数据信息的有效检验，进一步确保计算机网络信息安全应用总体目标。

4 计算机网络信息安全防火墙技术应用

4.1 访问加密

黑客入侵都是计算机网络信息安全普遍威胁之一，不但危及互联网信息安全性，也会对用户导致不良影响。可是防火墙技术可以根据计算机系统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。防火墙技术里最为中心的技术便是数据加密，在计算机网络信息安全管家运用，发挥出实用价值。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。全部进到计算机网络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[4]。

唯有输入正确登陆密码、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，非法侵入、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。从计算机网络信息安全角度考虑，非法侵入是比较常见的现象，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。

4.2 配置访问策略

对于防火墙开展设定环节中，需要对计算机运用有一个全方位了解，掌握原地址信息IP地址等信息，与此同时依据次序开展合理配置。根据被动安全环节中，防火墙技术的应用解决以下几个方面进行高度重视：

（1）就计算机网络来讲，主要包含许多类别的信息。运用防火墙技术能够对这种信息开展深入分析及梳理，对各种信息开展存档解决，融合每个部门及应用的差别，采用里外维护方式，全方位降低信息开展传送过程中产生的风险。（2）依靠合理方式。能通过防火墙开展检验，获得站点安全认证，对各个网站安全性能开展剖析，依靠合理的方法，可以全方位增强网络使用效率。（3）开展网站漏洞扫描。对计算机开展更新以后，依靠防火墙技术，能够对系统漏洞开展自查，同时还可以对用户开展提示，让他们第一时间处理相关问题[5]。

4.3 防火墙修复技术

在互联网时代，越来越多信息充溢到计算机网络中，同时通过计算机网络针对信息进行各种各样实际操作。针对用户来讲，并非所有的数据信息都是有用的数据信息，针对信息的监管并不像专业技术那样分类整理地开展获得或解决，这不仅会到在其中发生很多各种垃圾信息，进而也能给故意侵略者以废弃物信息搞混方式侵略的可能性。应用防火墙的修复技术，根据网络视频监控方式对用户全部获得的信息进行筛选并建表，根据用户的实际要求，针对废弃信息开展过虑，执行适度的合乎设定的阻拦或是删掉解决。这样一来，能够防止计算机网络侵略的同时还可以节约计算机的内存空间，与此同时也会提高用户计算机网络浏览及数据处理方法效率。根据防火墙修复技术的应用，提升了网络视频监控实际效果，针对有可能被运用各种垃圾信息开展及时的监测和解决，针对计算机网络安全生产环境的构建具有很重要的作用。

4.4 防火墙防护技术

防火墙的安全防护理论是主要是针对计算机网络中所最流行的木马程序的不良影响而运用的。木马程序要在计算机网络使用次数逐年递增的情形下，还在快速发展的一种互联网损害方式。用户根据计算机去进行网页访问或是针对存放在空间数据库中信息进行获得或操作时，有可能被潜藏在网站上或者存在某一些应用软件里的木马程序所损害。所以在用户开展网址访问或者互联网数据操作等行为情况下，防火墙全是处在开启状态下的，针对找到的异常数据信息故意损害个人行为将进行及时地鉴别，进而做出阻拦并拒绝访问的处理方法[6]。

4.5 包过滤防火墙技术的应用

包过虑防火墙要以互联网技术为载体，归类和装包解决计算机端口号、数据信息、详细地址等相关信息，接着根据实时监控系统计算机网络连接状态、数据文件等，立即鉴别数据文件和计算机网络全面的安全隐患，并分辨数据文件是否合适，一旦数据文件与设定要求相符合，数据信息才可以在应用系统中允许其行驶。相反，难以被信赖的数据文件会隔离在计算机网络系统软件外界，为此装修隔断各种进攻对计算机网络全面的损害。总而言之，在包过虑防火墙技术应用场景中，很有可能容许根据数据文件，也有可能把这些数据文件防护在设备外界，或是实行别的更复杂操作，可以有效提升计算机网络信息安全标准。

5 结束语

在计算机网络安全中，防火墙技术可以有效地改进全部计算机网络的安全性，为确保计算机网络的正常运转打下基础。文中阐述了防火墙的应用优势与重要性，根据防火墙技术的特点和发展趋向，有针对性地明确提出优化措施，进而能够更好地健全防火墙技术的安全系数，合理降低用户在使用中碰到的信息安全隐患，预防各种互联网恶意攻击所产生安全隐患。

参考文献

[1]董毅，汪安祺.大数据环境下的计算机网络信息安全防护对策[J].信息记录材料，2021，22（06）：22-23.

[2]李辉.大数据环境下计算机网络信息安全的对策研究[J].信息记录材料，2021，22（05）：44-46.

[3]赵强.基于计算机网络安全中防火墙技术的实践研究[J].网络安全技术与应用,2021(09):10-11.

[4]龚雨雄.网络信息安全与防火墙技术研究[J].电子测试,2021(16):127-128.

[5]巫飞龙. 防火墙技术应用于计算机网络信息安全中的策略探究[J]. 智库时代，2020(28):164-165.

[6]张馨蕊. 论防火墙技术在计算机网络安全中的应用[J]. 电脑编程技巧与维护，2021(1):161-163.