# 基于计算机网络的防火墙技术及实现

李剑
贵阳职业技术学院　贵州　贵阳　550081

[摘　要]随着科学技术的不断进步，我国开始逐渐步入互联网时代，计算机网络不仅仅成为人们口中的谈资，对其进行应用的范围也越来越广，现在各行各业的发展都离不开计算机网络，各个行业领域的发展方向也都趋向于信息化，而且计算机网络技术的广泛应用也为企业带来了更多的经济收益，为我国经济社会的快速发展提供了助力，但值得注意的是，在新的时代背景之下，计算机网络带给人类便利的同时，计算机网络技术仍然存在一定的弊端，那就是非常容易遭到具备一定技术的不法分子的入侵，会造成个人信息失窃，甚至会导致人们的财产受到一定的损失，正因如此，防火墙技术应运而生，防火墙技术能够有效防止计算机网络被入侵，能够保护好用户的个人以及企业的信息安全，本文将基于计算机网络的防火墙技术及实现的过程进行研究和讨论，以供参考。

[关键词]计算机网络；防火墙技术；应用
【DOI】10.12252/j.issn.2096-627X.2021.11.1299

## 引言

在新的互联网信息时代背景之下，人们已经开始逐渐习惯信息技术带来的便利，手机、平板电脑以及笔记本电脑成了人们生产生活当中必备的设备，而计算机网络是信息进行有效传输的基础，因此计算机网络一方面要保证信息传输的速度，确保信息具有时效性，另一方面也要保障信息在传输过程中的安全，因此必须要对计算机网络进行一定程度的防护，防火墙技术是目前经常使用的一类计算机网络防护技术，这一技术成本较低，但是使用效果较好，希望防火墙技术能够不断地更新优化，使之成为先进的计算机网络防护技术。

## 一、网络防火墙基本原理概述

所谓的防火墙技术通俗来讲就是一种能够应用在计算机网络当中，这种方式能够保护计算机网络在运行的过程中不会被恶意的入侵或者被破坏，能够有效保障计算机网络长时间安全稳定运转。一般的防火墙技术都是由软件和硬件组成，也就是访问服务政策系统、计算机安全检测系统、过滤系统以及网管系统。防护墙技术根据其应用方式的不同可以分为两大类，第一类防火墙技术被称为计算机防火墙技术，主要作用是将计算机与外部网络隔开，确保网络的恶意病毒等信息不会进入到计算机当中；第二类计算机技术被称为网络防火墙技术，主要作用于外部网络与计算机内部网络之间，确保计算机内部网络安全不受侵犯。在计算机网络运行的过程中，防火墙能够实时对计算机网络进行安全保障，会对外界网络传输进来的信息进行检测，过滤，确认无误后让信息通过防火墙进入到计算机内部网络，而一旦防火墙检测到外界传输的信息存在恶意入侵行为，防火墙将会立即启动隔绝系统，将计算机内部网络进行保护，与外界恶意入侵信息隔开，确保计算网络安全不被入侵，保障人们的信息安全。

## 二、常见防火墙技术种类

1.包过滤技术。包过滤技术是发明时间最长的一种防火墙技术，最开始的包过滤技术是一种相对静态的包过滤技术，这一技术通常作用于计算机网络，经过科学技术的发展，逐渐衍生出另一种动态的包过滤技术，这一技术在计算机网络之上还增加了一层防护，包过滤技术工作的目的是连接各类数据包，这是进出计算机网络的关口，包过滤技术将网络层和防护层作为实时监测的目标，对经过的每一个数据包进行全面的检测、过滤，要对数据包中的发送地址、签约协议、数据端口进行全面的检测分析，并且将分析得到的数据结果与提前设定好的防火墙过滤标准进行匹配，如果发现某一个数据包中与防火墙过滤标准匹配结果不符，则不能通过，那么传输过来的数据包将无法通过防火墙进入到计算机网络，会被隔离在计算机网络外围，如果传输过来的数据包与防火墙过滤标准匹配，则能顺利通过，那么这个数据包将会顺利地穿过防火墙进入到计算机网络当中，合理地设置好防火墙过滤标准能够有效提高防火墙的工作效率。但是包过滤技术的问题在于这一技术不具备智能化，只能按照提前设定好的标准进行过滤筛选，如果出现一个技术设计人员没有考虑到的危险数据传输过来，通过匹配就无法识别此危险数据，很有可能让危险的数据包进入到计算机网络当中。

2.代理服务技术。因为包过滤技术存在一定问题，导致无法为用户提供更为完善的计算机网络防护，因此在科研人员不断努力下，研发出了代理服务技术。代理服务技术通俗来讲就是形成一个数据传输通道，这一通道能够为用户访问进行保密，通常一个较为完善的代理设施需要有两个端口，分别是服务端口和客户端口，服务端口的作用是接收到用户操作的各类指令，然后服务端口会利用自身所具备的客户端口模拟器，将相应的数据传输回客户端口，这样就是一个完整的代理服务过程。而利用了代理服务技术的防火墙实质就是一个能够进行数据监测过滤的代理服务设备，然后防火墙将会应用协议分析，对传输进来的数据根据预先制定好的

标准进行分析，但是这已经不是单单按照标准来对数据进行匹配，而是根据防火墙过滤标准所提供的信息来对这些数据进行分析评估，可以判断出数据是否有技术设计人员没有考虑到的因素，并且能够对数据进行有效的隔离，从这一点上看，代理服务技术会比包过滤技术更加的先进和智能。

3.状态检测技术。这一技术是基于包过滤技术以及代理服务技术的基础上研发出来的，防护墙状态检测技术应用一种状态监视的插件，在保证计算机网络安全运行的基础上能够对计算机网络信息传输中的各个环节进行抽样检测，然后依照各类防火墙过滤标准来自行作出判断。状态检测技术在对数据包中的发送地址、签约协议、数据端口进行全面的检测分析的基础上还增加了一项对话过滤功能，在数据与计算机网络形成链接之后，防火墙技术会在链接当中建立一个对话的状态，在这一状态当中能够对数据所包含的全部信息进行检测，并且状态检测技术的特点在于第一次形成对话状态之后，在后续的数据传输过程中都会依照第一次的会话状态进行检测，如果之后的数据传输与第一次数据对话状态不相符，那这一数据就会被隔离在计算机网络之外，并且这样对话状态只会维持较短的时间，如果超过了一定的时间还没有更多的数据传输的话，那么这个对话状态将会被关闭。状态检测技术能够对数据内的信息进行分析，这一功能就是对原有的防火墙技术的更新优化，而且状态检测技术不需要有过多的数据连接端口，进而能够更好地保证计算机网络的安全。

## 三、目前计算机网络所面临的威胁和安全隐患

计算机网络是指能够通过一些计算机设备，例如智能手机、电脑等与互联网连接，然后做到对各类软件的使用和管理，还能够在现行网络传输规范标准的要求下，实现对信息数据传输的一种计算机系统，随着各类信息技术的不断更新换代，计算机网络所面临的威胁和安全隐患也在不断地更新换代，计算机网络主要面临的威胁有两类，一是黑客的恶意攻击，二是计算机病毒入侵计算机网络，这两类威胁能够损害的范围也在逐步地扩大，不仅能够直接攻击相应的计算机设备，还能够对互联网以及相关的信息进行攻击。

## 四、计算机防火墙技术的实现过程

1.网络地址转化技术。目前网络地址转化技术是防火墙最为重要的一项技术，这一技术就是利用防火墙将计算机网络的地址进行更改，通过这样的技术操作能够让计算机网络接收信息的地址更加的隐蔽，这样能够有效地对计算机网络进行保护，而且网络地址转化技术分为两类，第一类网络地址转化技术是不更改接收数据的地址，而是更改数据发送的起始地址，这样在进行转换的时候能够隔绝外部网络的干扰，这样就能够有效避免黑客的恶意入侵，而第二类网络地址转化技术就是不改变数据发送的起始地址，对接收数据的网络地址进行改变，而且在接收地址改变的时候不会更改数据发送和接受的原地址。

2.加密技术。加密技术也是会分为两类，一类是防火墙对称加密技术，这一类防火墙技术会比较常用，这一技术是在信息被传输之前对其进行加密，经过加密之后的信息在传输的时候就能够较好地保证不会被其他人恶意窃取，而且通过对称加密之后信息外层的密码解密难度不大；第二类技术是防火墙不对称加密技术，这一技术复杂程度较高，但是对信息的保护性会更好，这一加密技术就是对所要传输的数据进行加密之后，其密码可以进行全面公开，但是只知道这一密码是无法获取内部信息的，必须还要获取另一个密码，两个密码共同解锁，利用这两类加密技术能够非常有效地避免数据信息在传输过程中被他人恶意盗取，有效地避免了数据的损失。

3.多级过滤技术。第一级别的过滤就是对数据的来源地址以及假的数据接收地址进行过滤，能够筛选出真实的数据信息来源和接受的地址，网络关口过滤就是对计算机主机与外部互联网进行连接点进行监控过滤。通过过滤技术，能有效保障人们的信息不受侵害，在一定程度上也保障了信息更加安全。

## 结束语

综上所述，随着计算机技术的快速发展，防火墙技术一方面要对计算机主体进行有效保护，而且还要对数据传输过程进行保护，通过加密、过滤等多种方式实现对计算机网络的保护。本文笔者根据自身工作经历对防火墙技术的种类以及当前背景下计算机所面临的威胁进行了分析，并且提出一些计算机网络防火墙应用的方式，以期这些研究能给从事计算机工作的同仁启示，继续进行对防火墙技术的研究创新，提出更好的防火墙技术，维护我国互联网信息的安全，保护个人和企业信息不受侵犯。

## 参考文献

[1]高岳.基于计算机网络的防火墙技术及实现[J].科技资讯，2020，18（12）：12-13.

[2]陈前军.Solaris系统NAT和防火墙技术在计算机网络机房中的实现[J].电脑编程技巧与维护，2011（04）：67-68+70.

[3]玄文启.基于计算机网络的防火墙技术及实现[J].中国科技信息，2010（20）：117-118.

[4]赵磊.基于计算机网络的防火墙技术及实现[J].电脑迷，2016（12）：9.

[5]龚俭，杨望.计算机网络安全导论[M].南京东南大学出版社：202009.507.