设计研究与应用

基于计算机网络的防火墙技术及实现

许岩
（甘肃有色冶金职业技术学院，甘肃金昌 737100）

摘 要：人类的生活与工作越来越离不开电子计算机网络，而电子计算机网络的发展，一方面给人类生活提供了巨大的便利性，另一方面却也产生了一些安全问题。此外，网络安全运维的人员目前必须明确网络安全维护的基本操作步骤和保护技能要领，通过充分整合计算机的整个运作状态来为修补计算机的安全漏洞，为提高计算机的平稳运行重要技术保障。在当前，由于计算机技术的迅速发展，计算机网络的使用范围也愈来愈广泛，行业内都把信息化发展视为未来产品发展的大趋势，其中计算机网络的广泛应用也为众多产品提供了难以忽略的经济效益。但是在这一历史背景下，计算机网络又处在高风险的环境当中，既要避免计算机网络遭受侵犯，同时又要保障个人、公司等信息系统的安全，因此本文基于计算机网络的防火墙关键技术以及实现方式展开深度探讨，并给出个人建议，以期提供参考依据。

关键词：计算机网络；防火墙技术；实施
中图分类号：TP393.08 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2022.09.049
本文著录格式：许岩.基于计算机网络的防火墙技术及实现[J].软件,2022,43(09):169-172

Firewall Technology and Implementation Based on Computer Network

XU Yan
(Gansu Nonferrous Metallurgy Vocational and Technical College, Jinchang Gansu 737100)

【Abstract】：Human life and work are increasingly inseparable from the electronic computer network. The development of the electronic computer network, on the one hand, provides great convenience to human life, on the other hand, it also produces some security problems. In addition, the personnel of network security operation and maintenance must be clear about the basic operation steps and protection skills of network security maintenance at present. By fully integrating the entire operation state of the computer, they can repair the security loopholes of the computer and provide an important technical guarantee for improving the stable operation of the computer. At present, due to the rapid development of computer technology, the use of computer networks is becoming more and more extensive. The industry regards the development of information technology as the general trend of future product development, and the wide application of computer networks has also provided many products with economic benefits that can not be ignored. However, under this historical background, the computer network is also in a high-risk environment. It is necessary to not only avoid the computer network from being infringed, but also ensure the security of personal and corporate information systems. Therefore, this paper conducts in-depth discussion based on the key technologies and implementation methods of the computer network firewall, and gives personal suggestions to provide reference.

【Key words】：computer network;firewall technology;implementation

0 引言

自从计算机技术问世和网络社会的形成，高速发展的科学技术促进了现代化网络构建，深刻影响了人类的生产生活和信息交流，已经变成了生活中不可缺少的一部分。人们利用网络信息技术冲破了时间局限和距离限制，不仅完成了不同地区之间的信息即时通讯，而且广泛应用于工业生产领域，还能够大大提高生产率水平，由于互联网科技兴起，计算机技术在行业中使用也显得日趋普遍，并建立了相应的网络标准，为分布管理、信息交流与共享等创造了更加优越的环境。众所周知，计算机具有信息共享性、分布式广泛性、结构开放式等特征，所以，它也必然地会面临着信息系统的易碎性，使

作者简介：许岩（1985—），男，辽宁沈阳人，硕士研究生，研究方向：计算机软件与理论、计算机网络、无线传感器网络。

之面临着很大的安全问题。

1 现阶段中国互联网所面临的重大危险和问题

在剖析由于互联网网络的防火墙及其关键技术问题之前，本文先对现阶段对于互联网网络所产生的危险及其带来的隐患做出相应的阐述，并由此来寻求现代网络安全防火墙科技的实施走向。我们所说的互联网，就是指可以随时使用计算机设备和外部设备，或者经过网络链接在一起，以便进行对网络及其有关软件的管理和运行，以及在某些关于信息通信使用的法律规定规范和管理之下，可以进行信息资源传播与共享的计算机系统。而计算机的系统安全则是指在计算机网络工作流程中，为保证网络系统没有遭遇到来自外部的非法的系统攻击、侵入等技术问题的信息发送。而对计算机系统安全的保障则通常包括两个方面，分别为保障网络的时效性、完全性、保密性的安全保护，和避免计算机设备遭受来自外部的（火灾、水灾、爆炸等）损害的物理安全保障。

2 对于防火墙技术的概述

防火墙技术就是指广泛应用于计算机网络，以保护计算机网络在应用过程中不遭受非法入侵的技术手段，现代网络安全防火墙一般由硬件与软件组成，如业务接入政策、测试控制系统、包过滤器、应用网关技术等构成。在计算机设备与外网相互之间的防火墙称之为计算机与网络防火墙，而建立在国外互联网设施与国内网络相互之间的网络安全防火墙则被叫做网络防火墙 [1]。在正常工作时，防火墙会对由外部传出的消息加以监管、隔离，在被监测消息中不存在恶意信息同时被引入到内部的网络系统中，而一旦消息出现了攻击动向，防火墙就会对消息加以隔离，以保证内部计算机网络的安全性。如图 1 所示。

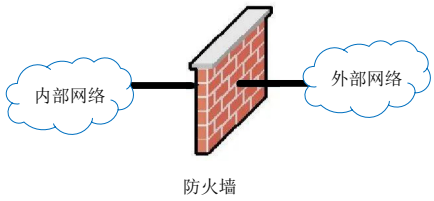

图 1 防火墙技术简易图

Fig.1 Simple diagram of firewall technology

3 防火墙技术的特性

防火墙的英文名称为 FireWall，也是目前一种最主要的互联网防御设备。从专业角度来说，防火墙是指处于两个（或多个）计算机网络之间，实现计算机与网络间访问控制的一个组件集合。

（1）国内网络系统和国外网络系统相互之间的任何互联网数据信息流都需要经过防火墙；这是由于防火墙所占的网络技术地位特点，同样还是一种前提条件。因为，唯有当网络安全防火墙是内、外网络系统间通信的唯一途径时，才能够更全面、有效地保障整个企业网部网络不受影响。因为网络安全防火墙的一端直接连通了事业单位内部结构中间的电脑局域网，而另一端则连通了因特网。所以在企业内、外互联网间的数据通信，都要经过网络安全防火墙，可见防火墙的重要性。

（2）只有具备安全保护措施的数据流才使用网络防火墙；网络防火墙最根本的作用就是保证了网络流量的有效性，并在此情况下把互联网的所有数据包迅速地从一个链接中转送到了其他的链接上。现从最初的网络防火墙模式出发说起，最初的网络防火墙是指一个双穴主机，即同时拥有两个网络连接，并具有两种网络层地址。网络防火墙首先把互联网上的所有数据包从合适的网络连接收集起来，然后沿着 OSI 协议栈的七层架构依次传递，对相关的网络层实施了使用规范的检查，进而把合乎通行要求的报文从合适的网络连接中发送出，但对一些不合乎通行要求的报文则进行了拦截。所以，从这种观点上来看，网络防火墙系统实际上是一种相似于桥接或网络路由器式的、多终端的（网络连接≥ 2）交换装置，其跨接在几个相互隔离的物理网段中间，并在报文的交换环节中进行对报文内容的审核操作。

（3）防火墙系统自身就应该具备相当强的抗进攻免疫力，这是防火墙系统之所以能够承担公司内部安全保护重担的重要前提。网络安全防火墙控制系统位于互联网边界上，它就像是一个边界警卫一般，每时每刻都要应对着黑客的进攻，这就需要网络安全防火墙控制系统自己也要具备相当强大的抵御进攻本事。它能够具备这么强大的本事，对网络安全防火墙控制系统自己也是至关重要，因为唯有与自己具备完全信赖关联的操作系统，这样才能够谈论整个网络系统的安全。

4 防火墙的种类

4.1 网络级防火墙

网络的防火墙也被叫做包过滤式防火墙，该类别的防火墙是指工作在消息发送地与消息收到地之间，对消息进行检测并执行隔离和通过指令的防火墙。现阶段我们使用的路由器是比较常见的局域网型防火墙，当数据经过路由器后，路由器能够通过对数据的检查结果作出数据的接收和转发命令，不过路由器的缺点是无法对数据的来源和去向做出检查。

4.2 应用级网关

这种类型的防火墙，还需要面对比较特殊的网络数据问题，对网络数据包检测的同时还需要进行过滤，针对数据包中的信息内容进行分类并录入，最后生成完全可信的数据报表 [2]。该类别的防火墙针对计算机网络的保护程度比较高，这主要归功于应用网关针对数据管

理、监控。

4.3 电路级网关

电路级网关另外一个叫法，即电缆级网关，电路级网关一般是当在两台或多台的个人电脑设置中间初次构建起 TCP 链路时，就会形成的一个防火墙屏蔽。电路级网关还会对与已形成网络连接的计算机设备间的消息交换进行监视，并通过对消息的监视检测是否有非法消息的传送或者接受，以便于对计算机设备作出接收和隔离消息的命令。

5 防火墙的体系结构

5.1 双宿主机模式

双宿主服务器模型是最简单的一个防火墙体系结构，该模型是环绕着至少拥有两个互联网连接的堡垒服务器而构建的。双宿主主机内部的所有网络系统都能和双宿主主机进行通信，但是在内部网络间却不能进行通信（不能直接转发）。

5.2 屏蔽主机体系结构

双重宿网络主机架构实现了国内外联网系统与对外联网系统间的营业（但是路由封闭），屏蔽网络主控架构，则通过一组单独的路由器来实现与国内外联网系统电脑间的营业。在这个结构中，大多数的安全机制由各种数据包过滤体系来进行（比如阻止人类绕过代理服务器直接连接外部网络）[3]。数据包过滤技术能够将国内互联网上的某台服务器变成堡垒主机，堡垒服务器处在内部互联网中，并被待上网的服务器使用的唯一的国内互联网服务器。

5.3 屏蔽子网模式

由于利用周边网阻隔，壁垒路由器能够避免外部互联网对壁垒路由器的攻击。在 DMZ 中壁垒路由器能够成为唯一的可访点，提供支持与用户通信并成为应用网关代理。对确定的能够直接向 Internet 上打开的任何应用领域，它也能够直接把该应用领域服务器置于 DMZ 上[4]。有两种屏蔽路由器，它们设在 DMZ 和内联网之间，或者在 DMZ 和外网之间，如果袭击者要攻入这个结构的内部网，需要同时经过两个网络路由器。

6 防火墙技术的实现过程

在对防火墙技术的基本类型做出介绍之后，接下来我们谈谈基于计算机网络的防火墙技术实现流程。

6.1 网络地址转换技术

当前网络安全防火墙技术发展中较为主要的手段就是互联网 IP 地址转变科技，而互联网 IP 地址转变科技顾名思义就是利用风火墙将国内互联网的 IP 网址加以改变，这样就能够在很大程度上隐藏消息收到的位置，进而对国内安全产生防护效果[5]。除此以外，互联网 IP 地址转变科技中包括两类，即 SNAT 和 DNAT，这两类的互联网 IP 地址转变科技针对 IP 网址的变化对象也有所不同。SNAT 则是不改变接收网址的情形下，直接改变数据信息的来源位置，并以此完成与国内网的交流，从而对外部网完全遮蔽，这样一来便能够在很大程度上提高国内互联网骇客进攻的困难[6]。但是 DNAT 却恰好和 SNAT 完全相反，因为 DNAT 实际是不改变数据信息包源地址范围的具体情况下，直接对数据信息包的接收地点作出了改变，而在位置转移流程中并不是对数据信息包所发送或者接受的最初地点作出改变。

6.2 加密技术

防火墙信息加密也可分成两类，它们是对称信息加密和非对称信息加密技术。其中，对称加密技术比较常见，它是指对需要传递的消息在传递之前进行加密，或者收到消息之后采用同样的密码进行解密，或者通过对消息加密从而确保在消息传递过程中没有被其他人所盗取，同时对称密码用同样的密码进行加密、破解，处理起来也更为方便[7]。而非对称的加密比较复杂，但是保密性也更高，而非对称密码则是指对需要传输的信息在进行保密后，密码就可向别人进行公布，因而该密钥也称为公开秘钥，但要想解开秘密并获取正确信息则还必须另一个秘密，即破解密钥[8]。利用上述两种加密技术，可以有效地防止其他人从消息传递过程中获得，从而给用户带来一定的经济损失。

6.3 多级过滤技术

在上文对网络安全防火墙关键技术方面做出了简要的说明，包括应用网关系统和电路网关系统等均采用了滤波技术，如图 2 所示。但这两种网络安全防火墙所选用的过滤技术级别一样是三层过滤技术。

这里一层滤波技术是通过对数据消息的源地址和假冒的接收位置加以筛选，以保证数据消息的传送和接收位置准确；而应用网关第一层则是对透过互联网所发生的情报交流、资源共享等服务事件实施监视滤波[9]；电路网关第一层过滤则是对服务器设备和对外互联网站点

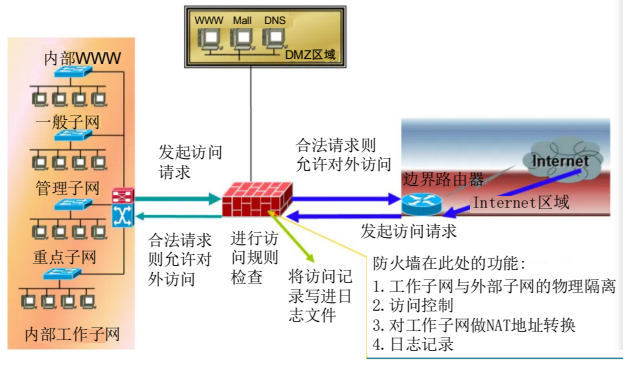

图 2 防火墙在过滤技术中的作用

Fig.2 The function of firewall in filtering technology

相互之间的渗透联系实施监听。

7 结语

综上所述，随着信息科技的蓬勃发展以及计算机与网络科学技术的日益完善，在当前人类的生活中计算机与网络将扮演着十分关键的角色，同时也将直接影响到世界经济社会的和平安定与我国的经济社会发展。在这个情形下，加强计算机技术系统安全的必要性不言而喻。要及时针对当前的状况来制定具体的调整计划，对当前的信息系统加以完善，提供具体的预防措施，切实保证当前计算机系统安全技术的有效提高，促进国家经济社会的稳定增长与经济社会的和谐。由于计算机网络技术的蓬勃发展，运用网络进行信息资料的交换、资源共享已成为当今社会的重要趋势。而现代防火墙技术不但要对计算机主机进行防护，而且还要对数据的传送进行严格保密，以此保证计算机间信息资料交换、数据共享的安全，但同时需要随着互联网科技的发展而进一步提升与完善。总之希望通过对计算机网络的防火墙技术不断探讨，能更好地保护企业及用户的信息安全，促进网络技术的不断健康持续发展，从而为人们提供更加便捷、安全的网络环境。

参考文献

[1] 龚俭,杨望.计算机网络安全导论[M].南京:东南大学出版社,2020.

[2] 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.

[3] 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.

[4] 叶碧野.基于计算机网络的防火墙技术及实现[J].数字技术与应用,2011(12):250-251.

[5] 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(4):67-68+70.

[6] 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.

[7] 唐怡.基于角色访问控制策略的防火墙技术研究与实现[D].长春:吉林大学,2005.

[8] 王钦国.计算机网络安全与防火墙技术分析[J].集成电路应用,2022,39(4):162-163.

[9] 王根.计算机网络安全技术发展与防火墙技术探讨[J].网络安全技术与应用,2022(3):6-7.

•••••• 上接第165页

证等技术的，支持动态口令、身份令牌以及指纹、指静脉和虹膜、人脸等多种认证因子的统一身份认证系统。该系统面向政府部门应用服务多、部署范围广、安全要求高的强身份认证需求，在技术层面领先开展了政务应用身份认证体系统一化尝试，依托既有的 PKI 密码证书机构和注册机构以及配套的证书申请、制发等密码服务基础设施，采用国产化操作终端、服务器和认证网关等安全设备，集成了公文传输、即时通信、重大决策监督、会议管理、资产管理、人事财务管理和档案管理等业务应用系统，为各应用系统提供了统一的用户身份管理和身份认证服务，为国家和地区政务系统的安全运行提供了有力可靠的支撑。

本文技术方案中的外部服务的实现主要基于该政务平台计算机专网项目的实际需求，对于其他特殊应用场合一般不具有普遍适用性，通常需要根据具体需求在实现方法上进行适当改造。相应的访问接口也还没有形成为行业内普遍认可的行业标准，未来在外部服务的设计方法和接口的标准化等方面还可以开展更多的研究工作。

参考文献

[1] YANG Y J.The Design of Unified Identity Authentication and Single Point Login System[J].Applied Mechanics and Materials,2012(155–156):391–395.

[2] GRUBB M F,CARTER R.Single Sign-on and the System Administrator[C]//Proceedings of 12th USENIX Conference on System Administration.Boston,1998: 63–86.

[3] 彭勇,黄剑华,王喆,等.分布式协同统一身份认证平台的设计与实现[J].软件工程,2020,23(10):52-54+41.

[4] 王群,李馥娟.一种基于单点登录的实验室统一身份认证方案[J].实验技术与管理,2020,37(5):219-223.

[5]张富友,王琼霄,宋利.基于生物特征识别的统一身份认证系统研究[J].信息网络安全,2019(9):86-90.

[6] 陈怡丹,李馥娟.数字证书安全性研究[J].信息安全研究,2021,7(9):836-843.

[7] BURIRO A.Behavioral Biometrics for Smartphone User Authentication[D].Trento: University of Trento,2017.

[8] 李中,龚俊,周加谊.基于麒麟系统下指纹识别系统设计研究[J].电子设计工程,2018,26(4):184-187+193.

[9] 王超楠,郭慧杰,韩一梁,等.基于虹膜识别的智能信息管理平台设计[J].数字通信世界,2019(12):92-93.

[10] 徐睿,游佳,刘坤,等.基于国密算法和PUF的企业用户身份认证系统[J].计算机与现代化,2018(3):102-107.