北 京 华 夏 管 理 学 院

毕 业 论 文

文 理 学 院 计 算 机 专 业

课 题 名 称 浅谈防火墙技术在计算机网络安全中的应用

学 生 姓 名 孙苗

学 生 班 级 计算机

指 导 老 师 付春霞

起 讫 日 期 2011。2—2011.4

2 0 1 1 年 4 月 2 3 日

防火墙在网络安全中的应用

摘　要

随着计算机网络技术的飞速发展，尤其是互联网的应用变得越来越广泛，在带来了前所未有的海量信息的同时,网络的开放性和自由性也产生了私有信息和数据被破坏或侵犯的可能性，网络信息的安全性变得日益重要起来,已被信息社会的各个领域所重视。本文对目前计算机网络存在的安全隐患进行了分析，阐述了我国网络安全的现状及网络安全问题产生的原因,对我们网络安全现状进行了系统的分析，并探讨了针对计算机安全隐患的防范策略。

正是因为安全威胁的无处不在，为了解决这个问题防火墙出现了。防火墙是网络安全的关键技术，是隔离在本地网络与外界网络之间的一道防御系统,其核心思想是在不安全的网络环境中构造一个相对安全的子网环境，防火墙是实施网络安全控制得一种必要技术。本文讨论了防火墙的安全功能、体系结构、实现防火墙的主要技术手段及配置等.

关键词
网络安全/黑客/病毒/防火墙

Firewall Network Security Application

ABSTRACT

With the rapid development of computer network technology, In particular, the application of the Internet has become more and more extensive， In bringing an unprecedented mass of information at the same time, Open and freely shaped the network also had private information and data have been damaged or the possibility of violations of, Network information security has become increasingly important, has been the information society in all areas of the pie. This article exists on the current computer network security risk was analyzed, elaborated on China’s network security and network security status of the causes for our network security status of a systematic analysis， and discusses the security risks for computer preventive strategies。

It is precisely because security threats everywhere， the firewall in order to solve this problem emerged。 Network security firewall is the key technology is to separate the local network and external networks of a defense system, its core idea is in an insecure network environment to construct a sub-network environment of relative security， the firewall is to implement the network security controls were a necessary technique。 This article discusses the firewall security features, architecture， to achieve the main technical means and firewall configuration。

key words
network security / hacking /virus/ firewall

目 录

1 引言

现今社会随着计算机网络技术的发展,促进了信息技术的变革，社会对计算机网络的依赖也逐渐增强.计算机网络正改变着人们在工作和生活中的方式.但是，随之而来的计算机网络受攻击现象也就出现了,数据丢失、网上银行账号密码被破解等现象，使用户苦不堪言，损失的也无法挽回。为保护计算机、服务器和局域网资源受到攻击等,利用防火墙技术是当前比较可行的一种网络安全保护技术。

2 我国网络安全现状

2.1 研究背景

据美国联邦调查局统计，美国每年因网络安全造成的损失高达 75 亿美元。据美国金融时报报道，世界上平均每 20 分钟就发生一次人侵国际互联网络的计算机安全事件，1/3 的防火墙被突破。美国联邦调查局计算机犯罪组负责人吉姆·塞特尔称：给我精选 10 名“黑客”,组成小组，90 天内,我将使美国趴下。一位计算机专家毫不夸张地说：如果给我一台普通计算机、一条电话线和一个调制解调器，就可以令某个地区的网络运行失常。

据了解，从 1997 年底至今，我国的政府部门、证券公司、银行等机构的计算机网络相继遭到多次攻击。公安机关受理各类信息网络违法犯罪案件逐年剧增，尤其以

电子邮件、特洛伊木马、文件共享等为传播途径的混合型病毒愈演愈烈.由于我国大量的网络基础设施和网络应用依赖于外国的产品和技术，在电子政务、电子商务和各行业的计算机网络应用尚处于发展阶段，以上这些领域的大型计算机网络工程都由国内一些较大的系统集成商负责。有些集成商仍缺乏足够专业的安全支撑技术力量，同时一些负责网络安全的工程技术人员对许多潜在风险认识不足。缺乏必要的技术设施和相关处理经验,面对形势日益严峻的现状，很多时候都显得有些力不从心。也正是由于受技术条件的限制，很多人对网络安全的意识仅停留在如何防范病毒阶段，对网络安全缺乏整体意识.

随着网络的逐步普及，网络安全的问题已经日益突。如同其它任何社会一样，互连网也受到某些无聊之人的困扰，某些人喜爱在网上做这类的事,像在现实中向其他人的墙上喷染涂鸦、将他人的邮箱推倒或者坐在大街上按汽车喇叭一样。网络安全已成为互连网上事实上的焦点问题。它关系到互连网的进一步发展和普及，甚至关系着互连网的生存。近年来，无论在发达国家,还是在发展中国家，黑客活动越来越猖狂，他们无孔不入，对社会造成了严重的危害。目前在互连网上大约有将近 80%以上的用户曾经遭受过黑客的困扰.而与此同时,更让人不安的是,互连网上病毒和黑客的联姻、不断增多的黑客网站，使学习黑客技术、获得黑客攻击工具变的轻而易举.这样，使原本就十分脆弱的互连网越发显得不安全。

2.2 研究意义

现在网络的观念已经深入人心，越来越多的人们通过网络来了解世界，同时他们也可以通过网络发布消息，与朋友进行交流和沟通，展示自己,以及开展电子商务等等。人们的日常生活也越来越依靠网络进行。同时网络攻击也愈演愈烈,时刻威胁着用户上网安全，网络与信息安全已经成为当今社会关注的重要问题之一.党的十六届四中全会，把信息安全和政治安全、经济安全、文化安全并列为国家安全的四大范畴之一，信息安全的重要性被提升到一个空前的战略高度。正是因为安全威胁的无处不在，为了解决这个问题防火墙出现了。防火墙的本义原是指古代人们房屋之间修建的那道为防止火灾蔓延而建立的墙，而现在意义上的防火墙是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称.应该说，在互连网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域(即 Internet 或有一定风险

的网络）与安全区域（局域网）的连接,同时不会妨碍人们对风险区域的访问。成而有效的控制用户的上网安全.防火墙是实施网络安全控制得一种必要技术，它是一个或一组系统组成，它在网络之间执行访问控制策略。实现它的实际方式各不相同，但是在原则上，防火墙可以被认为是这样同一种机制：拦阻不安全的传输流,允许安全的传输流通过。特定应用程序行为控制等独特的自我保护机制使它可以监控进出网络的通信信息,仅让安全的、核准了的信息进入；它可以限制他人进入内部网络，过滤掉不安全服务和非法用户；它可以封锁特洛伊木马，防止机密数据的外泄;它可以限定用户访问特殊站点，禁止用户对某些内容不健康站点的访问;它还可以为监视互联网的安全提供方便.现在国外的优秀防火墙如 Outpost 不但能完成以上介绍的基本功能，还能对独特的私人信息保护如防止密码泄露、对内容进行管理以防止小孩子或员工查看不合适的网页内容，允许按特定关键字以及特定网地进行过滤等、同时还能对 DNS 缓存进行保护.对 Web 页面的交互元素进行控制如过滤不需要的 GIF， Flash 动画等界面元素.随着时代的发展和科技的进步防火墙功能日益完善和强大,但面对日益增多的网络安全威胁防火墙仍不是完整的解决方案。但不管如何变化防火墙仍然是网络安全必不可少的工具之一。

2.3 计算机网络面临的威胁

2.3.1 网络安全脆弱的原因

（1)Internet 所用底层 TCP/IP 网络协议本身易受到攻击,该协议本身的安全问题极大地影响到上层应用的安全.

（2）Internet 上广为传插的易用黑客和解密工具使很多网络用户轻易地获得了攻击网络的方法和手段。

(3）快速的软件升级周期，会造成问题软件的出现，经常会出现操作系统和应用程序存在新的攻击漏洞.

（4）现行法规政策和管理方面存在不足。目前我国针对计算机及网络信息保护的条款不细致，网上保密的法规制度可操作性不强，执行不力。同时，不少单位没有从管理制度、人员和技术上建立相应的安全防范机制。缺乏行之有效的安全检查保护措施，甚至有一些网络管理员利用职务之便从事网上违法行为。

2.3。1 网络安全面临的威胁

信息安全是一个非常关键而又复杂的问题.计算机信息系统安全指计算机信息系

统资产（包括网络)的安全，即计算机信息系统资源（硬件、软件和信息）不受自然和人为有害因素的威胁和危害.

计算机信息系统之所以存在着脆弱性，主要是由于技术本身存在着安全弱点、系统的安全性差、缺乏安全性实践等; 计算机信息系统受到的威胁和攻击除自然灾害外，主要来自计算机犯罪、计算机病毒、黑客攻击、信息战争和计算机系统故障等。

由于计算机信息系统已经成为信息社会另一种形式的“金库”和“保密室”，因而，成为一些人窥视的目标。再者,由于计算机信息系统自身所固有的脆弱性，使计算机信息系统面临威胁和攻击的考验。计算机信息系统的安全威胁主要来自于以下几个方面:

（1）自然灾害.计算机信息系统仅仅是一个智能的机器，易受自然灾害及环境(温度、湿度、振动、冲击、污染）的影响。目前，我们不少计算机房并没有防震、防火、防水、避雷、防电磁泄漏或干扰等措施,接地系统也疏于周到考虑，抵御自然灾害和意外事故的能力较差。日常工作中因断电而设备损坏、数据丢失的现象时有发生。由于噪音和电磁辐射，导致网络信噪比下降，误码率增加，信息的安全性、完整性和可用性受到威胁。

（2)黑客的威胁和攻击.计算机信息网络上的黑客攻击事件越演越烈，已经成为具有一定经济条件和技术专长的形形色色攻击者活动的舞台.他们具有计算机系统和网络脆弱性的知识，能使用各种计算机工具.境内外黑客攻击破坏网络的问题十分严重，他们通常采用非法侵人重要信息系统，窃听、获取、攻击侵人网的有关敏感性重要信息,修改和破坏信息网络的正常使用状态，造成数据丢失或系统瘫痪，给国家造成重大政治影响和经济损失。黑客问题的出现，并非黑客能够制造入侵的机会，从没有路的地方走出一条路，只是他们善于发现漏洞.即信息网络本身的不完善性和缺陷，成为被攻击的目标或利用为攻击的途径，其信息网络脆弱性引发了信息社会脆弱性和安全问题,并构成了自然或人为破坏的威胁。

(3）计算机病毒。90 年代，出现了曾引起世界性恐慌的“计算机病毒”，其蔓延范围广，增长速度惊人，损失难以估计。它像灰色的幽灵将自己附在其他程序上，在这些程序运行时进人到系统中进行扩散。计算机感染上病毒后，轻则使系统上作效率下降，重则造成系统死机或毁坏，使部分文件或全部数据丢失，甚至造成计算机主板等部件的损坏。

(4）垃圾邮件和间谍软件。一些人利用电子邮件地址的“公开性”和系统的“可广播性”进行商业、宗教、政治等活动，把自己的电子邮件强行“推入”别人的电子邮箱,强迫他人接受垃圾邮件。与计算机病毒不同，间谍软件的主要目的不在于对系统造成破坏，而是窃取系统或是用户信息。事实上，间谍软件日前还是一个具有争议的概念，一种被普遍接受的观点认为间谍软件是指那些在用户小知情的情况下进行非法安装发装后很难找到其踪影，并悄悄把截获的一些机密信息提供给第下者的软件。间谍软件的功能繁多,它可以监视用户行为，或是发布广告，修改系统设置,威胁用户隐私和计算机安全，并可能小同程度的影响系统性能。

(5）信息战的严重威胁。信息战，即为了国家的军事战略而采取行动,取得信息优势,干扰敌方的信息和信息系统,同时保卫自己的信息和信息系统.这种对抗形式的目标,不是集中打击敌方的人员或战斗技术装备，而是集中打击敌方的计算机信息系统，使其神经中枢的指挥系统瘫痪。信息技术从根本上改变了进行战争的方法,其攻击的首要目标主要是连接国家政治、军事、经济和整个社会的计算机网络系统，信息武器已经成为了继原子武器、生物武器、化学武器之后的第四类战略武器。可以说，未来国与国之间的对抗首先将是信息技术的较量。网络信息安全应该成为国家安全的前提。

（6)计算机犯罪。计算机犯罪,通常是利用窃取口令等手段非法侵人计算机信息系统，传播有害信息，恶意破坏计算机系统，实施贪污、盗窃、诈骗和金融犯罪等活动.

在一个开放的网络环境中,大量信息在网上流动,这为不法分子提供了攻击目标。他们利用不同的攻击手段，获得访问或修改在网中流动的敏感信息，闯入用户或政府部门的计算机系统,进行窥视、窃取、篡改数据。不受时间、地点、条件限制的网络诈骗，其“低成本和高收益”又在一定程度上刺激了犯罪的增长。使得针对计算机信息系统的犯罪活动日益增多.

3 防火墙的安全功能及安全网络方案

3.1 防火墙具备的安全功能

防火墙是网络安全策略的有机组成部分，它通过控制和监测网络之间的信息交换和访问行为来实现对网络安全的有效管理。从总体上看,防火墙应该具有以下基本功能：

(1）报警功能，将任何有网络连接请求的程序通知用户,用户自行判断是否放行也或

阻断其程序连接网络。

(2）黑白名单功能,可以对现在或曾经请求连接网络的程序进行规则设置。包括以后不准许连接网网等功能。

（3)局域网查询功能,可以查询本局域网内其用户，并显示各用户主机名。

（4) 流量查看功能，对计算机进出数据流量进行查看，直观的完整的查看实时数据量和上传下载数据率。

(5)端口扫描功能，户自可以扫描本机端口，端口范围为 0-65535 端口，扫描完后将显示已开放的端口。

（6)系统日志功能，日志分为流量日志和安全日志,流量日志是记录不同时间数据包进去计算机的情况,分别记录目标地址，对方地址，端口号等.安全日志负责记录请求连接网络的程序,其中包括记录下程序的请求连网时间，程序目录路径等.

（7）系统服务功能，可以方便的查看所以存在于计算机内的服务程序。可以关闭，启动，暂停计算机内的服务程序.

（8）连网/断网功能，在不使用物理方法下使用户计算机连接网络或断开网络。

完成以上功能使系统能对程序连接网络进行管理,大大提高了用户上网的效率，降低的上网风险。从而用户上网娱乐的质量达到提高，同时也达到网络安全保护的目的.

3。2 网络安全的解决方案

3.2.1 入侵检测系统部署

入侵检测能力是衡量一个防御体系是否完整有效的重要因素,强大完整的入侵检测体系可以弥补防火墙相对静态防御的不足。对来自外部网和校园网内部的各种行为进行实时检测,及时发现各种可能的攻击企图，并采取相应的措施.具体来讲，就是将入侵检测引擎接入中心交换机上。入侵检测系统集入侵检测、网络管理和网络监视功能于一身，能实时捕获内外网之间传输的所有数据,利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并在数据库中记录有关事件,作为网络管理员事后分析的依据；如果情况严重,系统可以发出实时报警,使得学校管理员能够及时采取应对措施。

3.2。2 漏洞扫描系统

采用目前最先进的漏洞扫描系统定期对工作站、服务器、交换机等进行安全检查，并根据检查结果向系统管理员提供详细可靠的安全性分析报告，为提高网络安全整体

水平产生重要依据.

3.2。3 网络版杀毒产品部署

在该网络防病毒方案中，我们最终要达到一个目的就是:要在整个局域网内杜绝病毒的感染、传播和发作，为了实现这一点，我们应该在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段。同时为了有效、快捷地实施和管理整个网络的防病毒体系,应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能.

3。2。4 安全服务配置

安全服务隔离区（DMZ） 把服务器机群和系统管理机群单独划分出来， 设置为安全服务隔离区，它既是内部网络的一部分，又是一个独立的局域网，
单独划分出来是为了更好的保护服务器上数据和系统管理的正常运行。建议通过NAT（ 网络地址转换） 技术将受保护的内部网络的全部主机地址映射成防火墙上设置的少数几个有效公网IP地址。这不仅可以对外屏蔽内部网络结构和IP地址， 保护内部网络的安全，也可以大大节省公网 IP 地址的使用， 节省了投资成本.

如果单位原来已有边界路由器， 则可充分利用原有设备， 利用边界路由器的包过滤功能，添加相应的防火墙配置，这样原来的路由器也就具有防火墙功能了。然后再利用防火墙与需要保护的内部网络连接。对于 DMZ 区中的公用服务器,则可直接与边界路由器相连，不用经过防火墙.它可只经过路由器的简单防护。在此拓扑结构中,边界路由器与防火墙就一起组成了两道安全防线， 并且在这两者之间可以设置一个DMZ 区，用来放置那些允许外部用户访问的公用服务器设施。

3.2。5 配置访问策略

访问策略是防火墙的核心安全策略，所以要经过详尽的信息统计才可以进行设置在过程中我们需要了解本单位对内对外的应用以及所对应的源地址、目的地址、TCP或UDP的端口， 并根据不同应用的执行频繁程度对策略在规则表中的位置进行排序，然后才能实施配置.原因是防火墙进行规则查找时是顺序执行的,
如果将常用的规则放在首位就可以提高防火墙的工作效率。

3.2。6 日志监控

日志监控是十分有效的安全管理手段.往往许多管理员认为只要可以做日志的信息就去采集。如： 所有的告警或所有与策略匹配或不匹配的流量等等,
这样的做法看似日志信息十分完善，但每天进出防火墙的数据有上百万甚至更多，所以，只有采集到最关键的日志才是真正有用的日志。一般而言,
系统的告警信息是有必要记录的，对于流量信息进行选择，把影响网络安全有关的流

量信息保存下来.

计算机网络安全方案设计并实现

1.桌面安全系统

用户的重要信息都是以文件的形式存储在磁盘上,使用户可以方便地存取、修改、分发。这样可以提高办公的效率，但同时也造成用户的信息易受到攻击，造成泄密。特别是对于移动办公的情况更是如此。因此，需要对移动用户的文件及文件夹进行本地安全管理,防止文件泄密等安全隐患。

本设计方案采用清华紫光公司出品的紫光 S 锁产品，“紫光 S 锁”是清华紫光“桌面计算机信息安全保护系统”的商品名称。紫光 S 锁的内部集成了包括中央处理器（CPU）、加密运算协处理器（CAU）、只读存储器(ROM）,随机存储器(RAM）、电可擦除可编程只读存储器（E2PROM）等,以及固化在 ROM 内部的芯片操作系统 COS（Chip Operating System)、硬件 ID 号、各种密钥和加密算法等。紫光 S 锁采用了通过中国人民银行认证的 SmartCOS,其安全模块可防止非法数据的侵入和数据的篡改,防止非法软件对 S 锁进行操作。

2。病毒防护系统

基于单位目前网络的现状,在网络中添加一台服务器，用于安装 IMSS。

（1）邮件防毒。采用趋势科技的 ScanMail for Notes.该产品可以和 Domino 的群件服务器无缝相结合并内嵌到 Notes 的数据库中，可防止病毒入侵到 LotueNotes 的数据库及电子邮件,实时扫描并清除隐藏于数据库及信件附件中的病毒.可通过任何 Notes 工作站或 Web 界面远程控管防毒管理工作,并提供实时监控病毒流量的活动记录报告。ScanMail 是 Notes Domino Server 使用率最高的防病毒软件。

(2)服务器防毒。采用趋势科技的 ServerProtect.该产品的最大特点是内含集中管理的概念，防毒模块和管理模块可分开安装。一方面减少了整个防毒系统对原系统的影响，另一方面使所有服务器的防毒系统可以从单点进行部署，管理和更新。

(3)客户端防毒。采用趋势科技的 OfficeScan。该产品作为网络版的客户端防毒系统，使管理者通过单点控制所有客户机上的防毒模块，并可以自动对所有客户端的防毒模块进行更新.其最大特点是拥有灵活的产品集中部署方式,不受 Windows 域管理模式的约束，除支持 SMS，登录域脚本，共享安装以外,还支持纯 Web 的部署方式。

(4)集中控管 TVCS。管理员可以通过此工具在整个企业范围内进行配置、监视和维