学科代码： 0101

学　　号： 090403010024

贵 州 师 范 大 学（本　科）

课　程　论　文

题　　目：安全网络环境的构建

——防火墙技术的现状及研究

学　　院： 经济与管理学院

专　　业：信息管理与信息系统

年　　级：2009 级

姓　　名： 罗小宇

指导教师： 王立伟（教授）

完成时间： 2012 年 5 月 22 日

安全网络环境的构建

——防火墙技术的现状及研究

罗小宇

摘要： 互联网发展至今已经从基本信息共享向电子商务、 网络应用、 电子政务等更为复杂的方面发展， 随着商业应用和政府办公的增加， 网络安全逐渐成为一个潜在的巨大问题， 其中也会涉及到是否构成犯罪行为的问题。 提及网络安全就会想到网络安全技术， 而在当前网络安全技术中防火墙技术可以称得上是保障网络安全的一种最有效的技术之一。 防火墙技术作为一种隔离内部安全网络与外部不信任网络的防御技术， 已经成为计算机网络安全体系结构中的一个重要组成部分。本文简要介绍了防火墙在网络信息安全中的重要作用 ，描述了防火墙的原理及分类 ，分析了构建防火墙时对防火墙的选择与设置 ，说明了防火墙的主要规则设置方法。 然后从实际出发， 描述防火墙技术的应用现状。 最后提出了面对网络安全问题以及构建安全网络环境应用防火墙所面临的挑战， 其中论述了防火墙在网络安全中起的重要作用以及应用需求 ，最后对该技术的未来发展进行展望，以期促进防火墙技术发展，实现安全网络环境的构建。

关键词： 防火墙；网络安全；包过滤；网关

Abstract: The Internet has been the development from the basic information sharing to electronic business, network applications, such as the electronic government affairs more complex development, with the commercial application and the increase of government office, network security has become a potential huge problems, which also can involve is a crime problem. Mention of network security think of network security technology, and in the current network security technology could be called firewall technology is to ensure the safety of network one of the most effective technical one. Firewall technology as a kind of isolation internal security network and distrust of the external network defense technology, has become a computer network security system structure of an important component. This paper briefly introduces the firewall in the important role of network information safety, describes the principle and classification of the firewall, this paper analyzes the constructing a firewall of the selection and for firewall Settings, and explains the main firewall rules set up method. And then from set out actually, describes the present situation of the application of firewall technology. Finally put forward the face the problem of network security and the construction of the security network environment application firewall challenges, which discussed the firewall in network security on important role as well as the application requirements, and finally, the future development of the technology was discussed, so as to promote the firewall technology development, realize the security of the network environment construction.

Key word: firewall; Network security; Packet filter; Gateway

0. 引言

科学技术的飞速发展， 人们已经生活在信息时代。 计算机技术和网络技术深入到社会的各个领域， 因特网把“ 地球村 ”的居民紧密地连在了一起。 近年来因特网的飞速发展， 给人们的生活带来了全新地感受， 人类社会各种活动对信息网络地依赖程度已经越来越大。在互联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与安全区域的连接，　同时不会妨碍人们对风险区域的访问。因此，防火墙的作用就是防止不希望的、　未授权的通信进出被保护的网络。在互联网的众多站点中，非常多的网站都是由某种形式的防火墙加以保护，这是对黑客防范最严密，　安全性较强切较有效的一种方式。　这不免使的一些不法之徒恶意利用有效的网络工具进行恶意攻击。　网络环境日益复杂，　安全问题接受的挑战越来越大越来越多的时候，　对防火墙技术需要有全面的认识。　因此了解其所处的现状以及优势和缺点，未来的展望就显得格外重要。

1.　防火墙技术的概述

防火墙是防范网络攻击最常用的方法，　从技术理论上看，　如今的防火墙经过了多年的不断改进 ，已经成为一种先进和复杂的基于应用层的网关，不仅能完成传统防火墙的过滤任务，同时也能够针对各种网络应用提供相应的安全服务。

1.1.　防火墙技术的基本思想

防火墙技术的基本思想是限制网络访问，　它把网络分为两个部分：　外部网络和受保护网络（内部网络）。　相比企业而言，　外部网络一般指的是 Internet　，而受保护网络一般指企业自己建立的　Internet　防火墙，放在受保护网络和外部网络之间，　如图1　所示

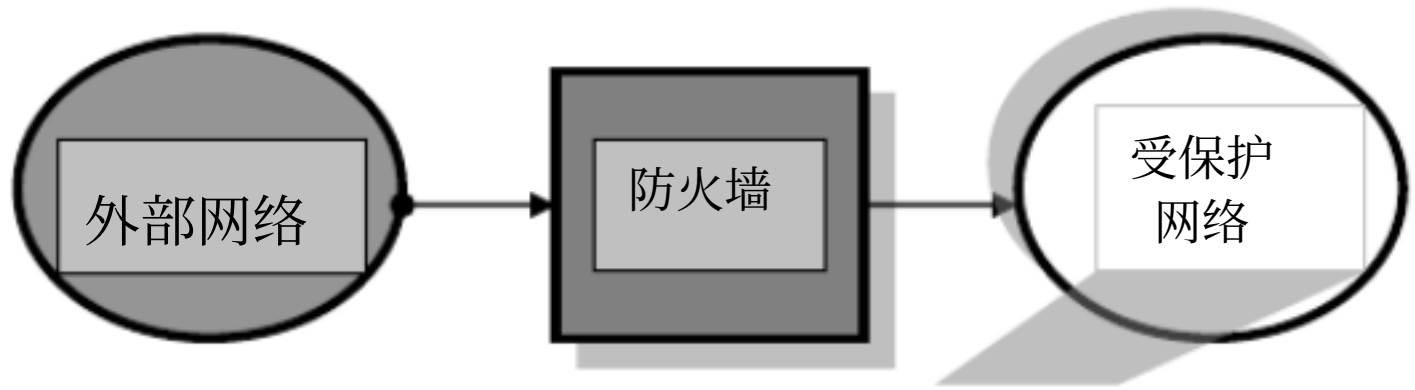

图 1.　政务网络方案图

资料来源：艾军　. 防火墙体系结构及功能分析　[M]. 江苏：江苏人民出版社　.2004.

防火墙一方面限制外部网络访问受保护网络，对外屏蔽受保护网络的实现细节，　保证数据的安全，　另一方面限制受保护网络对外部网络的访问，　防止不良信息的获取部分，减少信息的泄露。

1.2.　防火墙的工作原理

随着技术日益更新，　防火墙的种类也不仅仅局限与个别，　因此不同的防火墙具备不同的工作原理。　将不同的防火墙类型加以介绍，　可以帮助我们对防火墙原理的理解有更加深刻的认识。

1.2.1.　包过滤防火墙

包过滤防火墙一般在路由器上实现，用以过滤用户定义的内容，如　IP 地

址。包过滤防火墙的工作原理是：系统在网络层检查数据包，与应用层无关。这样系统就具 有很好的传输性能，可扩展能力强。但是，包过滤防火墙的安全性有一定的缺陷， 因为系统对应用层信息无感知， 也就是说， 防火墙不理解通信的内容，所以可能被 黑客所攻破。

1.2.2. 应用网关防火墙

应用网关防火墙检查所有应用层的信息包， 并将检查的内容信息放入决策过程，从 而提高网络的安全性。然而，应用网关防火墙是通过打破客户机／服务器模式实现的。 每个客户机／服务器通信需要两个连接： 一个是从客户端到防火墙，另一个是 从防火墙到服务器。另外，每个代理需要一个不同的应用进程，或一个后台运行的服务程序，对每个新的应用必须添加针对此应用的服务程序，否则不能使用该服 务。所以，应用网关防火墙具有可伸缩性差的缺点。

1.2.3. 状态检测防火墙

状态检测防火墙基本保持了简单包过滤防火墙的优点， 性能比较好， 同时对应用是透明的， 在此基础上， 对于安全性有了大幅提升。 这种防火墙摒弃了简单包过滤防 火墙仅仅考察进出网络的数据包，不关心数据包状态的缺点，在防火墙的核心部分建立状态连接表， 维护了连接， 将进出网络的数据当成一个个的事件来处理。可以 这样说，状态检测包过滤防火墙规范了网络层和传输层行为，而应用代理型防火墙则是规范了特定的应用协议上的行为。

2. 防火墙的构成及安全功能

概括的说， 防火墙的基本模型就是： 网络中继器和集线器是在最底层——物理层工作；交换机和网桥是在第二层———数据链路层工作； 路由器是在第三层——网络层工作。 防火墙建立在所有这些层上， 工作于第六层和第七层———会话层和应用层，这两层分别负责会话的建立、控制和应用。因此，通过防火墙，我们可以控制会话建立期间的所有信息流， 甚至可以决定当前的任何操作是否被允许。

2.1. 防火墙的基本构成

防火墙的基本构成包括：安全策略、高层认证、包过滤、应用网关。其中安全策略又分为扩展性策略、服务 / 访问策略、防火墙设计策略、信息策略、以及拔入与拔出策略。服务 / 访问策略是建立防火墙中最重要的组成部分，其余 3 部分在实现和执行策略中是必要的。 保护网站防火墙的有效性， 取决于使用防火墙的实现类型，以及使用正确的程序和服务 / 访问策略。

2.2. 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两大类型基本功能：

2.2.1.　当安全问题发生时应对的功能

防火墙的重要目标就是防范网络危害，　当危害发生时候要求防火墙能够提供

(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。

2.2.2.　针对具体的安全问题采取的措施

在这一阶段，防火墙需要做的除了上述所说的具体变现之外更为重要的就是有所作为。系统需要防火墙在报警等之外的功能之外还要做的更多，　比如记录危害的情况，对系统服务等。具体应该做的如下所述：

(1) 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。

(2) 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。

(3) 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。

(4) 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.　防火墙的应用现状

为了满足多样化的组网需求，　方便用户组网，同时也降低用户对其他专用设备的需求，减少用户建网成本，　防火墙上也常常把其他网络技术结合进来，　例如支持 DHCP SERVER、DHCP RELAY、支持动态路由，如　RIP　、OSPF 等；支持拨号、PPPOE 等特性；支持广域网口；　支持透明模式 (桥模式); 支持内容过滤 (如 URL 过滤) 、防病毒和 IDS 等功能。防火墙与其他安全设备或安全模块之间进行互动，

已经成为新一代防火墙的发展趋势。

3.1. 防火墙现状概述

防火墙的功能主要包含以下几个方面： 访问控制，如应用 ACL进行访问控制；攻击防范，如防止 SYNFLOOD等； NAT; VPN; 路由；认证和加密 ； 日志记录； 支持网管等。 此外为了保证可靠性， 支持双机或多机热备份； 为了满足日益增多的语音、视频等需求，对 QOS特性的支持和对 H.323、SIP 等多种应用协议的支持也必不可少。

但是，目前防火墙应用中的问题也不少。 如目前许多防火墙对内容过滤， 防病毒和 IDS 等的支持，实际的应用效果并不好。因为在这些功能支持的情况下，过滤会涉及到应用层包分析， 对 CPU的消耗很大。 这些功能的启动， 会导致性能急剧下降，本来 100M的处理能力，可能会下降到几兆，导致网络严重阻塞甚至瘫痪，失去了防火墙存在的意义。

3.2. 包过滤防火墙和代理

防火墙的发展， 经历了从早期的简单包过滤， 到今天广泛应用的状态包过滤技术和应用代理。 其中状态包过滤技术因为其安全性较好， 速度快， 得到最广泛的应用。应用代理虽然安全性更好， 但它需要针对每一种协议开发特定的代理协议，对应用的支持不够好。 从国外公开的防火墙测试报告来看， 代理防火墙性能表现比较差，因此在网络带宽迅猛发展的情况下，已经不能完全满足需要。

此外，有的防火墙支持 SOCK代理，这种代理屏蔽了协议本身，只要客户端支持 SOCK代理，该应用在防火墙上就可以穿越。这种代理对于部分不公开的协议，如 QQ的语音和视频协议，采用其他技术，在 NAT情况下很难实现对该协议的支持，但 QQ软件本身支持 SOCK代理，如果防火墙支持 SOCK代理协议，就可以实现对防火墙的穿越。 但对于防火墙而言， 不参与协议解码， 也意味着防火墙对该协议失去了监测能力。

3.3. 状态检测技术

状态检测技术最早是 CheckPoint 提出的，也就是要监视每个连接发起到结束的全过程。对于部分协议，如 FTP、H.323 等协议，是有状态的协议，防火墙必须对这些协议进行分析， 以便知道什么时候， 从哪个方向允许特定的连接进入和关闭。例如 FTP, 除了开始要建立命令通道外， 还要动态协商数据通道。 以 PORT方式为例， PORT模式下的工作过程如下：

(1) 客户端向服务器 21 端口发起连接，建立控制命令通道；

(2) 客户端向服务器发出命令，要求建立数据连接；

(3) 客户端打开一个端口；

(4) 客户端通过 PORT命令，从控制通道把端口号发给服务器；

(5) 服务器向客户端该端口发送一个主动连接。

从上述过程可以看出，客户端打开的端口号是未知的，所以防火墙必须对FTP控制通道的命令进行解码，从而知道协商后的端口号。然后，防火墙临时打开一个通道，允许服务器连接客户端的这个端口。对于状态防火墙，只需要通过ACL设置，开放该客户端对服务器的 21 端口连接。但对于以前的简单包过滤防火墙，如果想支持 PORT模式，还得对外开放所有的端口，这显然是不安全的。

状态防火墙可以对特定的协议进行解码，因此安全性也比较好。有的防火墙可以对 FTP、SMTP等有害命令进行检测和过滤，但因为在应用层解码分析，处理速度比较慢，为此，有的防火墙采用自适应方式，亦即根据当前防火墙繁忙程度做出判断：如果防火墙忙，则只做基本检测，如 FTP，只监测 PORT命令，其他有害命令就不检测，因此处理速度很快。

状态防火墙的抗攻击功能，还有一个特色是，当检测到 SYN FLOOD攻击时，会启动代理，此时，如果是伪造源 IP 的会话，因为不能完成三层握手，攻击报文就无法到达服务器，但正常访问的报文仍然可达。

3.4. 高保障防火墙

防火墙因为软件复杂，实现的功能较多，必须有操作系统支持，操作系统的安全是防火墙安全的基石。1998 年，在中国一家机构和美国计算机学会 ACM共同举办的国际会议上，我首次提出了高保障防火墙的概念，其核心是防火墙与安全操作系统无缝集成，在防火墙上实现类似 B级操作系统的机制，如标记、MAC强实体认证等。入关具有入关证，出关具有出关证。建立了防止内部敏感信息泄漏的机制，达到既防外又防内的目标，又实现了传统防火墙的全部功能。不久前，安胜防火墙应运而生，通过了国家权威机构的测评认证，是我国第一个研制成功的高保障防火墙，目前已经在我国 31 个省市广泛应用。

4. 防火墙技术在网络安全保护中的优势和不足

4.1. 防火墙所具备的优势

之所以在网络环境安全防范中防火墙越来越受到网络安全研究的重视，在于防火墙有其他设备无法比拟的优势。只要充分利用好其优点并发扬，将会给网络安全的建设带来不可想象的发展。

4.1.1. 防火墙能强化安全策略

因为在因特网上每天都有上百万的人浏览和交换信息，所以不可避免地会出现个别品德不良或违反因特网规则的人。防火墙是为了防止不良现象发生的“交通警察”，它执行网络的安全策略，仅仅允许经许可的、符合规则的请求通过。防火墙能有效地记录因特网上的活动。因为所有进出内部网信息都必须通过防火墙，所以防火墙非常适用收集网络信息。作为网间访问的唯一通路，防火墙能够

记录内部网络和外部网络之间发生的所有事件。

4.1.2. 防火墙可以实现网段控制

防火墙能够用来隔开网络中某一个网段， 这样它就能够有效地控制这个网段中的问题在整个网络中的传播。 防火墙是一个安全策略的检查点。 所有进出网络的信息都必须通过防火墙， 这样防火墙便成为一个安全检查点， 把所有可疑的访问据之门外。浙师大硕卜学位论文

4.2. 防火墙存在的不足

随着防火墙技术的发展， 其在信息安全体系中的地位越来越不可替代， 网络安全的严峻形势也对防火墙技术的发展提出了更高、 更新的要求。 在越来越依赖防火墙技术的情况下， 它对于一些特殊的攻击或其他行为有时也无能为力。 所以，我们也应该了解其技术方面的一些局限性， 毕竟没有任何一种技术能绝对保证安全。

首先，防火墙技术最突出的缺点在于不能防范跳过防火墙的各种攻击行为。这其中比较典型的就是难以防范来自网络内部的恶意攻击。 其次，防火墙技术的另外一个显著不足是无法有效地应付病毒。 当网络内的用户在访问外网中的含有病毒的数据时， 防火墙无法区分带毒数据与正常数据， 内部网络随时都有。 最后，防火墙的检测机制容易造成拥塞以及溢出现象。 由于防火墙需要处理每一个通过它的数据包，所以当数据流量较大时，容易导致数据拥塞，影响整个网络性能。严重时，如果发生溢出，就像大坝决堤一般，无法阻挡，任何数据都可以来去自由了，防火墙也就不再起任何作用。

5. 防火墙的发展趋势

可以预知， 未来防火墙的发展趋势是朝高速度、 多功能化、 更安全的方向发展。从国内外历次测试的结果都可以看出， 目前防火墙一个很大的局限性是速度不够。应用 ASIC 、 FPGA 和网络处理器是实现高速防火墙的主要方法， 其中以采用网络处理器最优， 因为网络处理器采用微码编程， 一般用户总希望防火墙可以支持更多的功能， 可以根据需要随时升级， 甚至可以支持 IPV6 ，而采用其它方法就不那么灵活。

实现高速防火墙， 算法也是一个关键， 因为网络处理器中集成了很多硬件协处理单元，因此比较容易实现高速。对于采用纯 CPU 的防火墙，就必须有算法支撑，例如 ACL 算法。目前有的应用环境，动辄应用数百乃至数万条规则，没有算法支撑，对于状态防火墙，建立会话的速度会十分缓慢。

受现有技术的限制， 目前还没有有效的对应用层进行高速检测的方法， 也没有哪款芯片能做到这一点。因此，防火墙不适宜于集成内容过滤、防病毒和 IDS 功能（ 传输层以下的 IDS 除外，这些检测对 CPU 消耗小 ） 。对于 IDS ，目前

最常用的方式还是把网络上的流量镜像到 IDS 设备中处理，这样可以避免流量较大时造成网络堵塞。此外，应用层漏洞很多，攻击特征库需要频繁升级，对于处在网络出口关键位置的防火墙，一般用户总希望防火墙可以支持更多的功能，如此频繁地升级也是不现实的。 多功能也是防火墙的发展方向之一， 鉴于目前路由器和防火墙价格都比较高， 组网环境也越来越复杂， 一般用户总希望防火墙可以支持更多的功能，满足组网和节省投资的需要。例如，防火墙支持广域网口，并不影响安全性，但在某些情况下却可以为用户节省一台路由器 ；支持部分路由器协议，如路由、拨号等，可以更好地满足组网需要 ；支持 IPSEC VPN，可以利用因特网组建安全的专用通道，既安全又节省了专线投资。

未来防火墙的操作系统会更安全。 随着算法和芯片技术的发展， 防火墙会更多地参与应用层分析，为应用提供更安全的保障。

6. 结束语

从目前防火墙产品及其功能上，可以看到防火墙的扩展功能将进一步完善，而且随着算法的优化，使对网络流量的影响减低到最少 IP。的加密需求越来越强，安全协议的开发是一大势点。 对网络攻击的检测和告警将成为防火墙的重要功能，将逐步建立和完善入侵检测数据库。 到目前为止， 新一代的防火墙采用信息安全技术，使得其功能更强大、安全性更强，可以抵御常见的网络攻击，如 IP 地址欺骗、特洛伊木马程序、 Internet 蠕虫、拒绝服务攻击等等。

但是，网络的安全是一种相对的安全， 目前还没有一种技术可以百分之百解决网络上的信息安全问题。 防火墙是一个确保网络安全的强大工具， 但是现有的防火墙有其局限性。 乐观的是：越来越多的大学院校和研究机构开始研究计算机与通信安全问题。我们相信，在不远的将来，肯定会出现全方位的“ 360 度”防火墙，这需要一代一代人不断的努力。

参考文献

[1] 艾军 . 防火墙体系结构及功能分析 [J]. 江苏：江苏人民出版社 .2004.

[2] 郑林 . 防火墙原理入门 [M]. 北京：北京大学出版社 .2006.

[3] 王卫平 . 防火墙技术分析 [M]. 上海：上海出版社 .2006.

[4] 孟涛，杨磊 . 防火墙和安全审计 [M]. 北京：电子工业出版社 .2004.

[5] 张宝剑 . 计算机安全与防护技术 [M]. 南京：机械工业出版社 .2003.

[6] 林海波 , 网络安全与防火墙技术 [M]. 北京：清华大学出版社 .2000.

[7] 凌雨欣 , 常红 . 网络安全技术与反网络入侵者 [M]. 武汉：冶金工业出版社 .2001.

[8] 王蓉 , 林海波 . 网络安全与防火墙技术 [M]. 北京：清华大学出版社 .2000.

致谢辞

在论文的写作过程中， 王立伟老师帮助了我很多。 虽然在这个过程中没有看过的稿子， 但是王老师课上的言传身教对我的影响非常之大。 另外还想特别表达感谢的是王老师这次论文作业要求， 开始或许会觉得非常的严格， 几乎不能出错，

又特别是对我们刚刚接触论文格式的大三学生而言。　　但是在这个过程中，　虽然十分的艰难，　完成论文那一刻的感受却是非常激动。　因为我们对明年的论文写作不再恐慌了，我们有底气面对了。尽量提前熟悉论文格式，了解写作的思路，知道选题等有关论文的要求想必才是王立伟老师的良苦用心。

所以，再一次的对王老师说一声谢谢。在你们的关心下，我会不断的努力，争取获得新的突破！学无止境　！这只是一个新的开始。

学生：罗小宇

时间： 2012 年 22 月