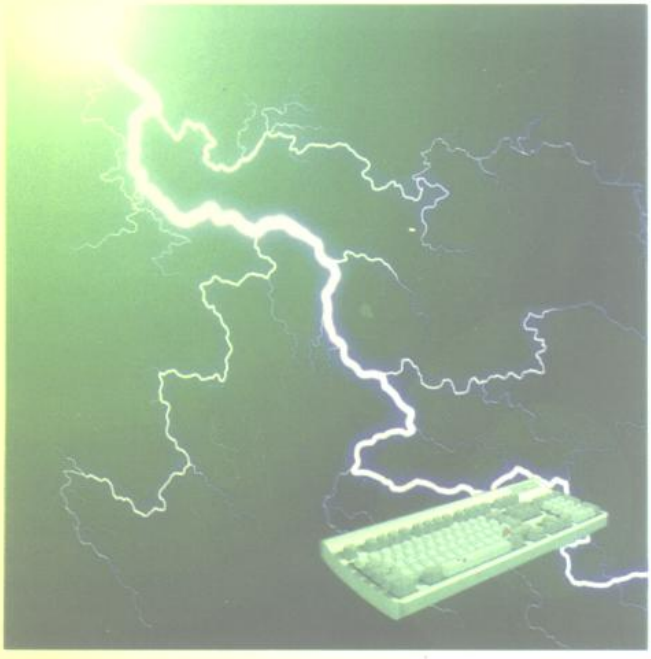
Network

网络软件与操作



计算机应用技术精华丛书

王仲文 主编
文宏武 副主编

本丛书是由首届全国计算机操作、编程、应用、维修有奖征文大赛的精华集粹而成。它突出实用性、启迪性，能起到举一反三，触类旁通的作用，是奉献给读者的“融理论与实践于一炉”的高质量的计算机应用技术丛书。

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL: http://www.phei.co.cn

计算机应用技术精华丛书

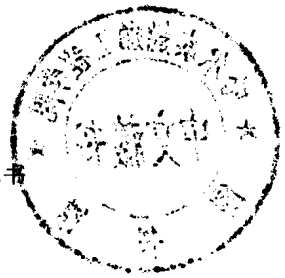
网络软件与操作

主　编　王仲文
副主编　文宏武

電子工業出版社
Publishing House of Electronics Industry

内容简介

本书取材于全国首届计算机操作、编程、应用、维修征文大奖赛，收集了其中有关计算机网络方面的优秀征文。其中包括 Internet 应用、网络操作系统及其互联技术、网络编程及实际应用等方面的文章，内容丰富多彩，极具参考价值，对从事计算机网络工作的专业人员及广大的爱好者很有帮助。



丛 书 名：计算机应用技术精华丛书

书　　名：**网络软件与操作**

主　　编：王仲文

副 主 编：文宏武

责任编辑：赵丽松

排版制作：电子工业出版社计算机排版室

印 刷 者：中国科学院印刷厂

出版发行：电子工业出版社出版、发行　URL：http://www.phei.com.cn

北京市海淀区万寿路 173 信箱　邮编 100036　发行部电话：68214070

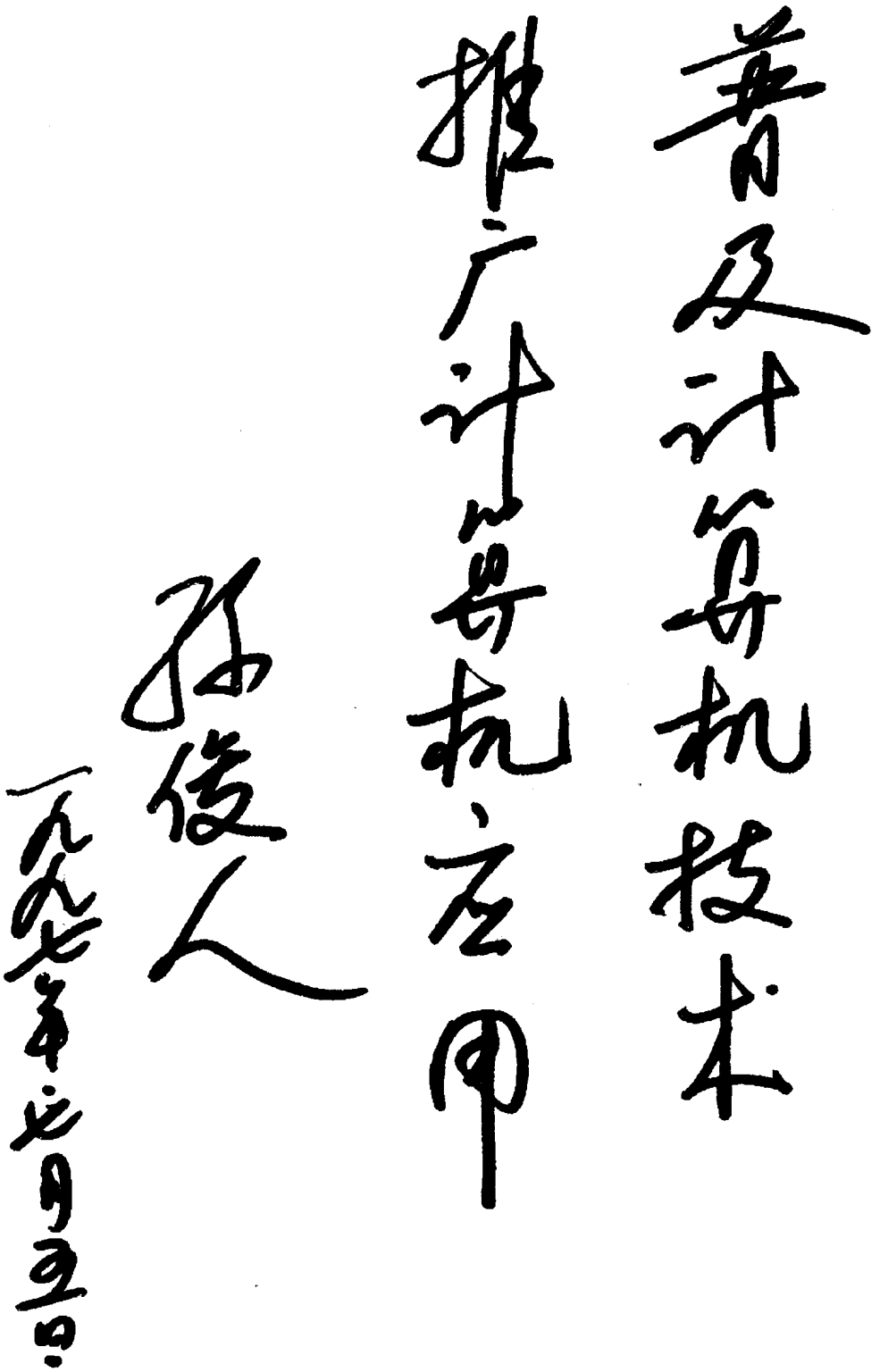
经　　销：各地新华书店经销.

开　　本：787×1092 1/16　印张：18.25　字数：460 千字

版　　次：1998 年 3 月第 1 版　1998 年 3 月第 1 次印刷

书　　号：ISBN 7-5053-4118-9
TP·1818

定　　价：24.00 元



中国电子学会理事长孙俊人工程院士的题词

编委会名单

主　任：梁祥丰

副主任：吴金生　胡毓坚　李新社　史新元

委　员：王　仪　王仲文　文宏武　邓露林　史新元　李　颖
李明树　李新社　杜国梁　宋瀚涛　许　远　赵　平
赵丽松　武　航　张务谦　张春晖　张祖荫　张　欣
吕再峰　杨丽娟　施玉新　胡毓坚　郭　立　高　平
梁祥丰　秦　梅　徐三南　龚兰方　程吉宽

评委会名单

主　任：李超云

副主任：李　颖　王明君　孙毓林　徐三南

委　员：王　仪　王仲文　王明君　文宏武　李明树　李超云
许　远　孙毓林　武　航　苏子栋　张务谦　张春晖
张祖荫　吕再峰　宋瀚涛　吴金生　杜国梁　高　平
秦　梅　徐三南　龚兰方　程吉宽

获 奖 名 单

二等奖

Internet 网安全问题与防火墙技术	王仲文
用 Windows Socket API 编制基于 TCP/IP 协议的网络数据传输程序	高守坤
Windows NT 与 UNIX 系统互联与实时通信	马占江

三等奖

用好 E-mail 电子邮件	何 渝
客户/服务器架构下的中间件技术	张 明
Internet 使用经验谈	王鉴、栾兆文
设计 Homepage 的若干认识	金尊和、张颍、贺新、陈淑君

出 版 前 言

为了普及计算机技术、推广计算机应用、迎接蓬勃兴起的全民学习计算机的热潮、总结广大计算机技术工作者、应用者、爱好者的技术成果以及在工作中的经验、体会、技巧，使之变为社会的财富。由电子工业出版社、中国计算机报社、中国计算机用户杂志社、中国电脑教育报社、软件世界杂志社共同发起组织的首届全国计算机操作、编程、应用、维修征文大奖赛，现在圆满结束。这次征文活动在读者中引起了强烈的反响，得到了广泛的响应，它有以下几个突出特点：

参与的普遍性，征文作者有计算机专业工作者，也有普通电脑使用者、爱好者、退休的老年人，还有在校的中学生。

内容的广泛性，来稿内容涵盖了计算机的各个技术领域。有开发项目完整的方案及程序设计，也有某个应用软件的使用技巧，还有硬件的防范及维护、维修经验。

文章的实用性，每篇文章阐述一个问题，讲深讲透，“拿来”就能用。

技术的先进性，来稿中包含了当前计算机的“热门”技术，如 Windows 95、Internet、多媒体及图形图象处理技术、Visual Basic、Visual C + + 等等。

从大量征文中经过主编认真遴选，编成《计算机应用技术精华丛书》——《数据库编程与应用(上、下)》、《网络软件与操作》、《多媒体与图形动画技术》、《办公软件实用技巧》、《操作系统及其使用技巧(上、下)》、《计算机语言及其应用实例》、《微机硬件故障防范与修复》共九种，现在正式出版发行。

应该说明的是：入选《计算机应用技术精华丛书》的文章就其技术性、实用性、先进性、可读性而言都是征文中比较优秀的。从入选《计算机应用技术精华丛书》的文章中经过由计算机专家组成的评委会评选出的获奖征文，其质量更胜一筹，相信《计算机应用技术精华丛书》的读者会有所鉴别。

征文活动的成功，《计算机应用技术精华丛书》的顺利出版，要感谢广大读者的热情参与、各册主编和各位评委的辛勤劳动。

发起组织征文大赛的初衷是重在参与，不以入选、获奖论英雄。入选、获奖的毕竟是少数，参与就是胜利！同时，由于篇幅所限，有的比较好的文章也未能入选，对此，除深感遗憾外，更要特别感谢那些积极、踊跃的参与者。

对于征文的组织、《计算机应用技术精华丛书》的出版，组织者们尽管尽心尽力了，但由于时间比较仓促，文章的挑选、编校的质量难免仍有疏漏，恳请读者指正。

目　录

第一部分

Internet

Internet 网安全问题与防火墙技术

北京电子科技学院　（100039）　王仲文

摘要：

本文首先分析 Internet 的不安全因素，诸如 IP 和 ICMP 协议弱点、认证的脆弱性、易监视性、易侦查性和易欺骗性等，然后详细论述了防火墙技术。

一、前　言

Internet 是一个以 TCP/IP 通信协议联接各个国家、各个机构计算机网络的数据通信网。Internet 网的前身是 ARPANET 网（美国军方计算机网络，由美国国防高级计划局于 1969 年牵头建立的）。Internet 网目前已普及到世界各地，据悉截止 95 年底该网拥有计算机 420 万台，拥有 4000 万用户，预计到 98 年用户将超过 1 亿，目前全球共有 92 个国家 50344 个计算机网络与 Internet 相联。据《美国新闻与世界报道》杂志 1995 年 11 月号介绍，至少有 250 万北美居民曾经通过 Internet 进行购物。我国 94 年 8 月正式与 Internet 相联，目前共有 5 条专线与 Internet 相联，速率从 64Kbps 到 256Kbps，97 年底个别线路将升为 1M ~ 2Mbps。据国家经济信息化联席办公室介绍，到 95 年底，国内有 1 万台计算机、6 万个用户入网。

随着计算机网络在我国的迅速发展，特别是与国际计算机网络互连后，网络系统的安全问题越来越受到重视。网络系统的安全对国家机关、企业、银行、科研机关、学校是至关重要的。然而绝对安全的网络是根本不存在的，也是不可能实现的。

美国国防部制定的“可靠计算机标准评估准则”（Trusted Computing Standards Evaluation Criteria）将计算机安全划分为四个级别（A ~ D），每个级别又细分为若干次级。其中 A1 为最高，若达到 A1 级标准，计算机存放地点绝对保密，又不加电，其它的计算机均达不到这个标准。一般的 UNIX 系统只有 log— in 口令和文件保护等几项安全措施被定为 C1 级，在 PC 机上运行的 DOS 则只被定为 D1 级，目前还很少有能够达到 B 级标准的计算机系统。网络安全，实际上也是指一定程度的安全，其安全程度要根据实际需要和所具备的条件而定。要求网络安全性越高，网络使用的限制越强。网络的安全性与网络的使用性是一对矛盾，必须根据实际情况兼顾两者。

前面介绍过，Internet 网是基于 TCP/IP 协议的国际性网络，讨论 Internet 安全问题，必须讨论 TCP/IP 的安全问题。目前，防火墙技术是保护 Internet 安全的常采用的技术，全球连入 Internet 的计算机中约有 1/3 是处于防火墙保护之下的。

本文在讨论 Internet 网的不安全性基础上，介绍防火墙技术。

二、Internet 网的不安全因素

网络安全性的含义是指:网络服务的可用性(Availability)、网上信息的完整性(Integrity)和保密性(Confidentiality)。就是说,从网络安全的角度来说,网上用户应实时得到各种网络服务,并且应能保证其信息完整、准确地传播。

首先,Internet 网是范围非常广的国际性网络,因其中间环节多,在所有网络中,其安全性是最低的;其次,Internet 网的技术协议 TCP/IP 本身存在着技术弱点,造成网络的不安全性。

Internet 采用 TCP/IP 连网协议,它是由 TCP、IP、UDP、ICMP 四个主要协议和其它 FTP、TELNET、SMTP、HTTP、PROTOCOL 等应用程序协议组成的。

TCP/IP 层从网络层次考虑(与 ISO 对照)由四个层次组成:应用层、传输层(TCP 层)、网络层(IP 层)和网络接口层。

应用层向用户提供一组常用的应用程序,如文件传输、电子邮件传递、远程登录等。当然用户也可以在 TCP 层上建立自己的专用程序。

传输层(TCP 层)提供应用程序之间的通信,即格式化信息流,并提供可靠地传输(接收端必须发回 Acknowledge 确认信息,信息丢失重发等)。为区别各应用程序,传输层在每一分组中增加了识别信源和信宿的信息,为确保传输正确还在每一分组中附加校验和项。

网络层(IP 层)负责相邻计算机间的通信。处理来自 TCP 层的分组发送请求(收到请求后,将分组装入 IP 数据包,填充报头,选择去往信宿的路径,后将该数据报交给网络接口层的适当的网络接口);同时处理来自网络接口层的输入数据包(首先检查其合法性,然后寻径。一旦该数据包到达信宿机,则去掉报头,交给适当的传输协议;如果尚未到达信宿,则转发该数据包);还要处理 ICMP 报文。

网络接口层是 TCP/IP 协议的最低层,负责接收 IP 包并通过网络发送;或者从网络上接收物理帧,分出 IP 包交给 IP 层。网络接口程序分为设备驱动程序和含自身数据链路协议的复杂子系统(如 X.25 中网络接口)。

由上面讨论的 TCP/IP 协议结构和功能层次,可以总结出 Internet 网络的几个不安全因素。

1. IP 协议的弱点

IP 包中的源地址项,标明该包是哪个主机上发出的,此外 IP 包中为测试目的设置一个选项,叫 IP Source Routing,该选项可以直接指明到达节点的路径,它是由一串所经过的 IP 节点地址组成的。TCP 和 UDP 会轻信此包是有效的,然而攻击者就可以利用这个选项进行欺骗,进行非法连接。例如,攻击者可以冒充某个可信用户的 IP 地址,构造一个通往某个服务器的源路由,指定通往该服务器的直接路径和返回的路径,利用可信用户作为通往服务器的路由中最后一站,就可以向服务器发请求,服务器信以为真,就将允许入侵者访问用户。

我们知道,UDP 在两个主机之间不建立虚电路,因而没有初始化的握手过程,所以 UDP 较 TCP 更容易被欺骗,所以风险更大。

2. ICMP 协议弱点

ICMP 的重定向信息可以欺骗路由器或主机,将正常的路由器定义为失效的路由器,从而可以帮助攻击者非法存取。

3. Internet 认证的脆弱性

Internet 没有口令认证，在 UNIX 操作系统中常常将加密后的口令存在一个普通用户就可以读的文件里。一旦得到这个口令文件，入侵者就可以运行早已准备好的口令破译程序去破译口令。

另外，一些 TCP 或 UDP 只能对整个主机地址而不是对指定用户进行认证。这样，系统管理员就无法区分该主机上的用户的可靠性，要么都授权，要么都不授权。

4. 易监视、易侦查性

当使用 Telnet 或 Ftp 时，从他自己的账户连接到另一台主机时，用户的口令是以不加密方式通过 Internet 的。这就给入侵者提供机会，入侵者可以监视含有用户各种口令的 IP 包，就会利用这个用户名和口令进行正常登录，进行非法连接。如果入侵进管理员的账户就会获得特权访问。有名的 SNIFFER 程序就是这种侦查入侵软件。

同样，用明文传送的电子邮件更易被监视，因为 SMTPS 是将邮件以 ASCII 码明文在 Internet 上传递的。

95 年 2 月 15 日被捕的计算机黑客凯文·米特尼克，在 Internet 上窃取了数以万计的数据文件和至少两万个信用卡号，所利用的技术就是 IP 地址欺骗。

5. 易欺骗性

在 UNIX 环境中，非法用户用 TCP/IP 将其 PC 机连接到 UNIX 主机上，将 UNIX 主机当做服务器，使用 NFS 对主机目录和文件进行访问，因为 NFS 只使用 IP 地址对用户进行认证。而将一台非法 PC 机用户设置成合法 PC 用户同样的名字和 IP 地址是非常容易的。

Internet 上的电子邮件特别容易受欺骗，因为一个入侵者可以很容易地将 Telnet 连接到一个系统的 SMTP(简单邮件传送协议)端口上，然后手工输入命令，收方主机相信发送方的主机就是所声称的主机，就可以轻易仿冒。例如，1995 年 7 月某天，麻省理工学院一个学生在弗罗里达通过 PPP 建立了一个与 Internet 连接的机器并错误地将其地址配置成麻省理工学院的地址。提供 PPP 服务的路由器将麻省理工学院的信息全部送往弗罗里达，同时还将路由信息同时通报给其它路由器，至使麻省理工学院与 Internet 中断联系半个小时。

三、防火墙的概念和作用

为了保护一个网络不受外来网络的攻击，确保本网络的安全，目前发展最快的技术是一种称为“防火墙”技术。这很象建筑物中为防止火灾漫延而设置的防火墙，不过在两个网络之间设置的防火墙确有本身特有目的。

设置防火墙的主要目的是保护内部网络，限制来自外部网络的访问，主要有以下内容：

1. 保护内部网络存在的某些脆弱服务

防火墙对通过它的某些协议可以进行限制，例如可以禁止 NFS 进出防火墙，只允许在网络内部使用，又如可以对路由器进行保护，防止 ICMP 重定向信息及带路由信息的 IP 包的攻击，使网络的某些脆弱服务得以屏蔽。

2. 控制外部网络对内部网络的访问

防火墙可以提供对节点的访问控制保护功能,不希望外部接入的节点可以很好地受到保护。

3. 便于内部网络安全的集中管理

如果从安全策略考虑需对内部网络集中安全管理时,防火墙便可以将一次口令技术、身份识别、密钥分配管理等功能集中起来,实现网络安全、信息加密的中心。

4. 隐藏内部网络的敏感信息,强化内部网络安全

对于内部网络的每个节点的敏感信息,如域名和 IP 地址,只对内部网络用户公开,而对外部网络入侵者则不容易利用其进行入侵。防火墙可以封锁诸如 Finger、DNS 等服务,断绝入侵者获这些敏感信息的来源。

5. 防火墙可以提供日志记录

如果能够对进、出内部网络的通信业务都记录下来;便于对通信业务进行分析,保证网络安全,防火墙可以实现此功能。

6. 执行网络安全政策

安全政策是受保护(内部)网络为自身安全目的,根据实际情况而制定的一系列规定、原则策略。防火墙可以集中体现这些安全政策,这是防火墙的重要功能。

现在可以叙述防火墙的概念了。防火墙是在内部网络(受保护网络)和外部网络(不安全网络)之间设置一个关卡点(Checkpoint),此关卡点对进出内部网络的通信业务进行安全检查,根据安全政策保护合法访问,限制非法访问,防止侵袭活动,防火墙示意图见图 1。

CHESWICK 和 BELLOWIN 两人曾对防火墙做了如下描述:

防火墙系统是置于两个网络之间的一种部件集合,它具有以下性质:

(1) 所有从内到外,或从外到内的通信业务都必须通过防火墙。

(2) 只有本地安全政策规定所允许的通信业务才能通过防火墙。

(3) 防火墙自身应是安全的、不可穿透的。

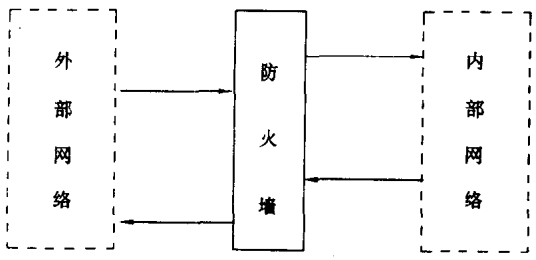


图 1 防火墙示意图

上述对防火墙的定义实际上可以用来描述几乎所有的网络安全设备的技术,如硬件加密设备、筛选路由器、堡垒主机或者应用层网关。这是一个极其通用的术语,为广大网络设备厂商和应用人员所接受。而学术界则认为防火墙应是完全不同于路由器的设备,是可以在应用

层对报文分组进行处理的网络安全设备，如双宿主机、应用层网关等；而把硬件加密设备、筛选路由器等工作在网络层以下的设备只看作防火墙的组成部件。按这种观点防火墙的模式型应如图 2 所示。

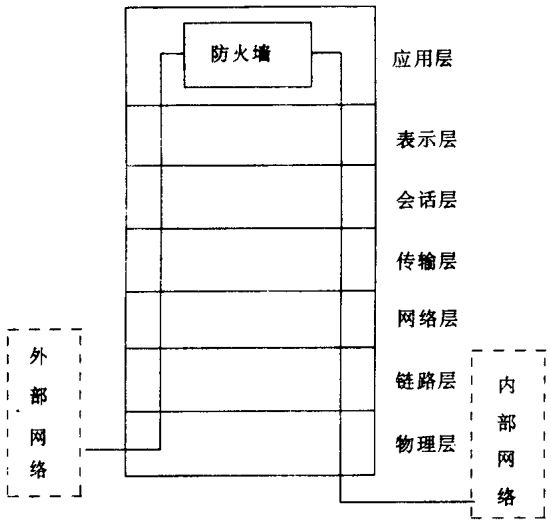


图 2　防火墙模型

在设计防火墙时，除了安全策略外，还要确定防火墙类型和拓朴结构。一般来说，防火墙被设置在可信赖的内部和不可信赖的外部网络之间。防火墙相当一个流控器，可用来监视或拒绝应用层的通信业务。防火墙也可以运行在传输层和网络层，这种情况下，防火墙检查进入和离去的报文分组 IP 和 TCP 头，根据领先设计的报文分组过滤规则来拒绝或允许报文分组通过。

防火墙是用来实现网络安全措施的主要设备。在许多情况下需要采用验证安全和增强私有性技术来加强网络的安全或实现网络方面的安全措施。

四、防火墙的基本构件

根据在网络上的物理位置和在 OSI 层模型中的逻辑位置，防火墙的组成构件可以分为两种，一种是包过滤构件(作用于 IP 层)，另一种是作用于应用层的网关式构件。

1. 包过滤构件

目前市场上可以购买到的具有包过滤功能的路由器就是最常见的这种部件，然而并不是所有的路由器都具有包过滤功能。

包过滤构件作用于 IP 层(如图 3 所示)，可以根据它所收到的每个数据包的源地址、目标地址、TCP/UDP 源端口号、TCP/IP 目标端口号、TCP/IP 包的各种标志位进行判决，根据一定的安全政策使数据包有选择地通过。

包过滤构件作用在 IP 层，感知信息有限，存在许多缺陷和不足。

(1) 不能够抵御包欺骗技术的袭击；

(2) 过滤规则复杂，正确性难以保证；

(3) 无审计功能，对非法包只是删除；

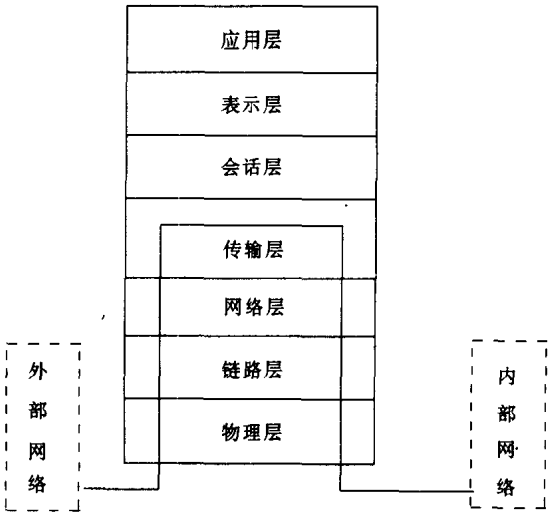


图 3 包过滤部件的服务位置

(4) 过滤作用局限,对动态指定 TCP 端口的应用协议无法有效过滤。

2. 作用于 TCP/IP 应用层的网关式部件

网关式防火墙部件作用于应用层上,因而安全控制会更精确。网关式防火墙中有应用代理服务功能,即有一个 Application Proxy(应用代理)模块,对到达此网关部件的应用请求进行处理。首先,对该用户的身份进行验证,若为合法用户,则把该请求转发给真正的某个内部主机(真正的服务提供者)。而且在整个服务过程中,应用代理一直监控着用户的行动,一旦发现用户的行动异常,即发出报警,请求管理员干涉,并对每一个活动作记录。若为不合法用户,则拒绝访问。图 4 给出网关式部件的服务位置,图 5 给出代理服务的示意图。

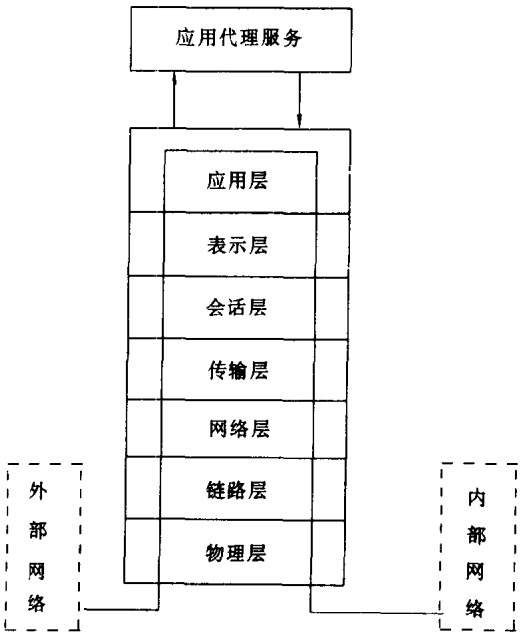


图 4 应用网关式部件的服务位置