全国高职高专计算机类“十二五”规划教材
网络安全工程师认证教材
校企合作开发教材

防火墙技术项目化教程

主　编　刘静　杨正校
副主编　刘坤　普星　沈啸　胡正好

西安电子科技大学出版社
http://www.xduph.com

全国高职高专计算机类“十二五”规划教材
网络安全工程师认证教材
校企合作开发教材

防火墙技术项目化教程

主　编　刘　静　杨正校
副主编　刘　坤　普　星　沈　啸　胡正好

西安电子科技大学出版社

内 容 简 介

本书是江苏省中高职衔接项目“基于校企共建专业的中高职衔接的研究与实践”的重要成果之一。本书共分两部分，其中基础理论篇围绕防火墙的概念与功能、工作原理、安全标准与评价体系、体系结构与分类、设计、防火墙技术的发展进行系统化概述；应用实践篇共 6 个项目，首先实现防火墙基本环境的搭建，然后进行 SNAT 等基本模式配置，在此基础上实现 DHCP 服务器等常用功能，针对上网行为从 Web 安全认证等方面实现过滤功能实操，完成防火墙 VPN 高级配置，最后参照省级、国家级技能大赛的要求进行网络安全系统综合训练。附录中给出防火墙配置常见命令。

本书可作为高职高专院校相关专业的教学用书，也可以为广大网络安全方面的专业技术人员及计算机爱好者提供参考。

图书在版编目(CIP)数据

防火墙技术项目化教程/刘静，杨正校主编. —西安：西安电子科技大学出版社，2015.3

ISBN 978-7-5606-3663-4

Ⅰ. ①防… Ⅱ. ①刘… ②杨… Ⅲ. ①计算机网络—安全技术—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 039067 号

策　　划　高　樱

责任编辑　马武装　王彦然

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西华沐印刷科技有限责任公司

版　　次　2015 年 3 月第 1 版　2015 年 3 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　　印　　张　12.5

字　　数　295 千字

印　　数　1～3000 册

定　　价　23.00 元

ISBN 978-7-5606-3663-4/TP

XDUP 3955001-1

前　言

随着网络技术的快速发展，移动互联和电子商务正在改变着人们的信息技术应用和生活方式，企业和个人越来越频繁地利用互联网进行交易，个人经常使用信用卡在网络上进行电子交易或贸易，不同公司之间也利用网络进行广泛的信息传递。互联网已经成为信息流和资金流的重要载体和传输渠道。个人隐私资料或企业的商业机密等信息一旦被非法网络入侵者拦截、修改或盗用，将存在严重的安全隐患。防火墙(Firewall)技术就是一种保护网络用户免受非法入侵，保证网络传输中的信息安全的技术。

防火墙是设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业安全策略控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。它是一种提供信息安全服务、实现网络和信息安全的基础设施。

本书是江苏省中高职衔接项目“基于校企共建专业的中高职衔接的研究与实践”的重要成果之一。本书作者联合行业企业和兄弟院校，共同开发教材资源，将行业信息安全管理经验与院校信息安全教学项目结合起来，依据防火墙工作原理和机制，选取行业经典防火墙应用技术案例，并融入省、国家信息安全技能大赛内容，以项目为载体组织教学内容，以任务为导向，突出防火墙应用技术能力训练。书中各项目和任务都从需求背景开始，突出真实性和实用性。

本书将理论与实践相结合，注重工作与学习的统一。本书一方面由浅入深地介绍了防火墙技术知识，给出了当前最新防火墙技术的开发与应用知识点，使读者能够较快掌握防火墙技术并能应用到实际中解决问题；另一方面，本书将防火墙实践操作技能通过 6 个项目导入，以企业真实任务为载体，采取由浅入深的方式组织技能训练项目，使读者在任务完成过程中逐步实现防火墙配置技能的螺旋式提升。书中实践项目中的前 5 个项目由若干任务组成。任务内容组织首先从防火墙简单的源 NAT、目的 NAT 等基本模式配置入手，然后结合防火墙的 DHCP 服务、DNS 服务等常用服务器功能配置，再将防火墙的多种安全过滤功能与其常用功能结合起来，最后进行防火墙 VPN 高级模式配置训练。每个任务后面都配有相关知识点链接和思考。每个项目后，均提供了项目实训。第 6 个项目为综合实训项目，实现由网络设备和多个防火墙、服务器构成的网络安全系统的部署。本书为高职高专的网络安全与管理类专业提供了实用教材，也可供本科以及网络安全技术人员参考使用。

本书由苏州健雄职业技术学院刘静副教授、杨正校院长主编，其所在专业团队教师全员参与了教材的编写工作。通过收集大量资料，经过 4 个学期的教学实践反复论证，并吸收防火墙应用的最新实用技术校企共建专业的合作相关方协同完成本书的编写工作。本书配有完整的 PPT 教学课件，方便广大教师参考使用。同时充分考虑高职高专学生的特点，设计了基础理论篇和应用实践篇，并在实践中进行理论知识链接，内容选取与操作通俗易懂，便于学生快速掌握防火墙应用技术。

本书得到江苏省教育厅的基金资助，苏州健雄职业技术学院教务处领导给予编写组很多的关心和支持，信息安全技术专业协作共建方——江苏省昆山第一中等专业学校、太仓市工投信息系统集成有限公司等为本书的编写提供了技术支持帮助，在此一并致谢！

由于作者水平有限，书中难免存在不妥之处，敬请读者批评指正。

作 者

2014 年 10 月 6 日

目　录

基 础 理 论 篇

第1章　防火墙的概念与功能 2
1.1　防火墙的概念 2
1.2　防火墙的功能 3
课后习题一 4
第2章　防火墙的工作原理 6
2.1　包过滤技术 6
2.2　应用代理技术 7
2.3　状态监视技术 8
课后习题二 8
第3章　防火墙的安全标准与评价体系 10
3.1　防火墙的安全标准 10
3.2　防火墙的评价体系 10
课后习题三 13
第4章　防火墙的体系结构与分类 14
4.1　防火墙的体系结构 14
4.2　防火墙的分类 16
4.2.1　软件防火墙 16
4.2.2　硬件防火墙 16
4.2.3　几种主要的防火墙 17
课后习题四 23
第5章　防火墙的设计 25
5.1　防火墙的设计规则 25
5.2　常见防火墙设计技术 25
5.3　常见防火墙的设计 27
5.4　防火墙实施方式 27
5.4.1　基于网络主机的防火墙 27
5.4.2　基于路由器的防火墙 28
5.4.3　基于单个主机的防火墙 29
5.4.4　硬件防火墙 29

课后习题五 31
第6章 防火墙技术的发展 33
课后习题六 34

应 用 实 践 篇

项目1 配置防火墙基本环境 36
任务1-1 使用CLI方式配置防火墙基本环境 36
任务1-2 使用WebUI方式配置防火墙基本环境 41
项目实训一 配置防火墙基本环境 44
项目2 基于防火墙的局域网与广域网的访问控制与实现 45
任务2-1 局域网访问广域网的控制与实现 45
任务2-2 同网段之间的访问控制与实现 51
任务2-3 广域网访问局域网的控制与实现 57
任务2-4 局域网、广域网与服务器的访问控制与实现 65
项目实训二 基于防火墙的网络访问控制实现 71
项目3 基于防火墙的网络配置与实现 73
任务3-1 防火墙DHCP服务功能与实现 73
任务3-2 防火墙DNS服务功能与实现 77
任务3-3 防火墙源路由服务功能与实现 81
任务3-4 防火墙负载均衡服务功能与实现 87
项目实训三 基于防火墙的网络服务功能实现 94
项目4 基于防火墙的信息过滤控制与实现 96
任务4-1 网络通信访问控制与实现 96
任务4-2 局域网带宽及应用访问控制与实现 99
任务4-3 Web安全认证控制与实现 105
任务4-4 网络通信软件访问控制与实现 113
任务4-5 网页地址过滤控制与实现 115
任务4-6 网页内容过滤控制与实现 119
项目实训四 防火墙过滤功能配置 123
项目5 基于防火墙的虚拟专用网(VPN)的访问控制与实现 125
任务5-1 静态路由虚拟专用网(IPSec VPN)的访问控制与实现 125
任务5-2 静态策略虚拟专用网(IPSec VPN)的访问控制与实现 138
任务5-3 远程安全访问虚拟专用网(SSL VPN)的访问控制与实现 151
项目实训五 防火墙高级模式配置 157
项目6 网络安全系统综合实训 159
附录 防火墙配置常见命令 172
参考文献 194

基础理论篇

随着网络技术的快速发展及其广泛应用，网络中出现的信息泄密、数据篡改和服务拒绝等安全事件频繁发生，网络安全问题越来越严重。为解决这些问题，出现了很多网络安全技术和方法，防火墙技术是应用最广泛也是最为成功的一种。

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用型安全技术，被广泛应用在专用网络与公用网络的互联环境中，特别是接入 Internet 的网络中。

第 1 章 防火墙的概念与功能

1.1 防火墙的概念

“防火墙”这个术语来自建筑结构安全技术。在建筑楼宇中，“墙”用来分隔不同的区域或房间，防火墙还具有防火隔离作用。一旦某个单元起火，这种隔离措施或方法将有效地保护其他居住者。多数防火墙上都有一个门，允许人们进入或离开，因此，防火墙在保护人们的安全、增强建筑的安全性的同时也允许必要的访问。在计算机网络中，防火墙是保护网络免受其他网络攻击的一个屏障。具体地讲，防火墙是一种用来加强网络之间访问控制的特殊网络设备，它按照一定的安全策略，对两个或多个网络之间传输的数据包和连接方式进行检查，从而决定网络之间的通信是否被允许，其中被保护的网络称为内部网络或私有网络，另一方则被称为外部网络或公用网络。防火墙能有效地控制内部网络与外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤不良信息的目的。

从技术实现角度来讲，防火墙是采用综合的网络技术，如包过滤技术等，设置在被保护网络(一般称为内网)和外部网络(一般称为外网)之间的一道屏障，用以分隔内部网络与公共网络系统，防止发生不可预测的、存在潜在破坏性的入侵。它是不同网络或网络安全域之间信息传递的唯一通道，像在两个网络之间设置了一道关卡，能根据企业的安全策略控制出入网络的信息流，防止非法信息流入被保护的网络，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

常见防火墙在网络中的拓扑结构如图 1-1 所示。

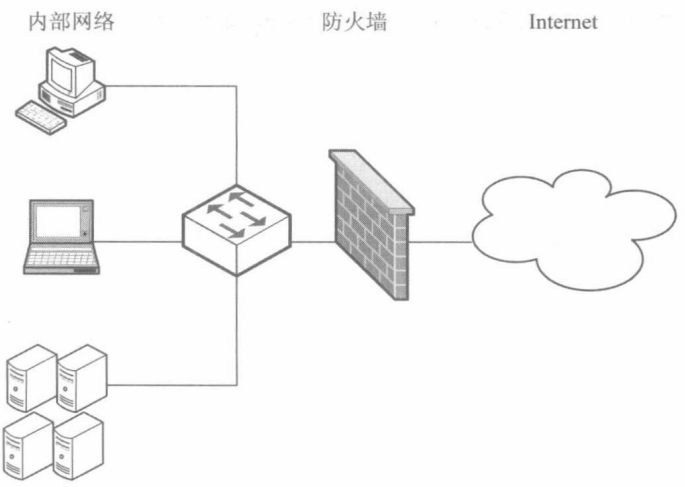

图 1-1 防火墙在网络中的拓扑结构

在防火墙结构中，连接外网的路由器(外部路由器)强迫所有流入的通信流量经过应用网关，而连接内网的路由器(内部路由器)仅仅接受来自应用网关的分组。实际上，网关控制着那些流入和流出内部网络的网络服务的传递。例如，防火墙只允许指定的用户连接到互联网，或者只允许特定的应用程序在内部主机和外部主机之间建立通信。如果被允许的服务是 E-mail，那么只有 E-mail 的分组被允许通过路由器。这样不但保护了应用网关，也避免了未经许可的分组太多而造成负荷过载。

1.2 防火墙的功能

如果没有防火墙，网络系统的安全只能依靠自身的安全设备和配置来保障，当这些安全设备系统升级或正在运行管理服务时，就可能处于不安全或不可信的状态，网络就很容易受到攻击；另外，这类安全设备可能使得网络只能从一个特定的位置来访问，从而使得网络系统功能没有发挥出来。如果没有防火墙，计算机安全就完全依赖于计算机自身，整个网络系统的安全将由系统中安全性最差的主机所决定，系统中只要有一台不安全的主机，就等于整个系统都处于不安全的状态之中，随着网络规模的增大，要把网络内所有的主机维护至同样高的安全水平是复杂的。更残酷的是，许多用户的计算机水平很差，根本不可能做到这一点，而且，若一时粗心就会因为简单的配置错误、遗漏或没有打安全补丁而导致整个网络系统或服务器系统被攻击。

当防火墙成为与不可信网络进行联系的唯一纽带后，管理员就不再需要确保每一台主机的安全，他只要集中关注、配置防火墙就行了。当然这并不是说防火墙里面的每个主机的自身安全就不重要了，即全部依靠防火墙的想法也是不对的，因为防火墙只是提供了一层避免错误的额外保护而已。

防火墙类似一名审计员，它记录了流经它的所有流量和访问日志，那些包含在日志中的信息可以用来重新构建新的事件以防安全出现缺口，同时可以用作事后查证。防火墙可以减轻系统被用于非法和恶意目的的风险，可以保证网络的安全。一般来说，防火墙可以防范一个网络或企业内的数据和信息在以下三方面的风险：

(1) 机密性的风险，包括某方未经授权就访问的敏感数据或数据的过早泄露。

(2) 数据完整性的风险，包括未经授权就对数据进行修改，例如财务信息、产品特性或某网站上商品的价格。

(3) 可用性的风险。系统可用性保证系统可以适时地为用户服务。

综上所述，防火墙具有以下作用：

(1) 保护脆弱的服务。通过过滤不安全的服务，防火墙可以极大地提高网络安全和减少子网中主机的风险。例如，防火墙可以禁止 NIS、NFS 服务通过，还可以拒绝源路由和 ICMP 重定向封包。

(2) 控制系统访问。防火墙可以提供对系统的访问控制，可以允许从外部访问某些主机，同时禁止访问另外的主机。例如，防火墙允许外部访问特定的 Mail Server 和 Web Server。

(3) 集中安全管理。防火墙对企业内部网实现集中的安全管理，在防火墙定义的安全规则可以运行于整个内部网络系统，而无需在内部网的每台机器上分别设立安全策略。即

防火墙可以定义不同的认证方法，而不需要在每台机器上分别安装特定的认证软件，外部用户也只需要经过一次认证即可访问内部网。

(4) 增强的保密性。使用防火墙可以阻止攻击者获取攻击网络系统的有用信息，如Finger和DNS。Finger显示了主机上所有用户的注册名、真实用户名，以及最后登录时间和使用的Shell类型等。

(5) 记录和统计网络利用数据以及非法使用数据。使用防火墙可以记录和统计通过防火墙的网络通信，提供关于网络使用的统计数据，并可以根据提供的统计数据来判断可能的攻击和探测。

(6) 策略执行。防火墙提供了制定和执行网络安全策略的手段。

课后习题一

一、选择题

1. 为控制企业内部对外的访问以及抵御外部对内部网的攻击，最好的选择是(　　)。
   A. IDS　　B. 杀毒软件　　C. 防火墙　　D. 路由器
2. 防火墙是指(　　)。
   A. 防止一切用户进入的硬件　　B. 阻止侵权进入和离开主机的通信硬件或软件
   C. 记录所有访问信息的服务器　　D. 处理出入主机的邮件的服务器
3. 防火墙能够(　　)。
   A. 防范恶意的知情者　　B. 防范通过防火墙的恶意连接
   C. 防备新的网络安全问题　　D. 完全防止传送已被病毒感染的软件和文件
4. 下面不是计算机网络面临的主要威胁的是(　　)。
   A. 恶意程序威胁　　B. 计算机软件面临威胁
   C. 计算机网络实体面临威胁　　D. 计算机网络系统面临威胁
5. 一般而言，Internet防火墙建立在一个网络的(　　)。
   A. 内部网络与外部网络的交叉点　　B. 每个子网的内部
   C. 部分内部网络与外部网络的结合处　　D. 内部子网之间传送信息的中枢
6. 在企业内部网与外部网之间，用来检查网络请求分组是否合法，保护网络资源不被非法使用的技术是(　　)。
   A. 防病毒技术　　B. 防火墙技术　　C. 差错控制技术　　D. 流量控制技术
7. 下列属于防火墙功能的是(　　)。
   A. 识别DNS服务器　　B. 维护路由信息表
   C. 提供对称加密服务　　D. 包过滤
8. 以下有关防火墙的说法中，错误的是(　　)。
   A. 防火墙可以提供对系统的访问控制
   B. 防火墙可以实现对企业内部网的集中安全管理
   C. 防火墙可以隐藏企业网的内部IP地址
   D. 防火墙可以防止病毒感染程序(或文件)的传播

二、简答题

1. 什么是防火墙？
2. 防火墙的主要功能有哪些？
3. 防火墙在网络拓扑中有什么作用？

第2章 防火墙的工作原理

传统意义上的防火墙技术分为 3 大类：包过滤(Packet Filtering)技术、应用代理(Application Proxy)技术和状态监视(Stateful Inspection)技术。无论一个防火墙的实现过程多么复杂，归根结底都是在这 3 种技术的基础上进行功能扩展。

2.1 包过滤技术

包过滤技术是最早使用的一种防火墙技术，它的第一代模型是静态包过滤，使用包过滤技术的防火墙通常工作在 OSI 模型中的网络层上，后来发展更新的动态包过滤增加了传输层。简而言之，采用包过滤技术的就是各种基于 TCP/IP 协议的数据报文传递的通道，该技术把这网络层和传输层作为数据监控的对象，对每个数据包的头部、协议、地址、端口、类型等信息进行分析，并与预先设定好的防火墙过滤规则进行核对，一旦发现某个包的一个或多个部分与过滤规则匹配并且条件为阻止的时候，这个包就会被丢弃。

适当地设置过滤规则可以让防火墙工作得更安全有效，但是这种技术只能根据预设的过滤规则进行判断，一旦出现一个没有在设计人员意料之中的有害数据包请求，整个防火墙就形同虚设了。人们也许会想，自行添加不行吗？但是别忘了，应该为普通计算机用户考虑，并不是所有人都了解网络协议，如果防火墙工具出现了过滤遗漏问题，用户只能等着被入侵了。一些公司采用定期从网络升级过滤规则的方法，这个方法固然可以方便一部分家庭用户，但是对相对比较专业的用户而言，却不见得就是好事，因为他们可能会根据自己的机器环境设定和改动规则，如果这个规则刚好和升级后的规则发生冲突，用户的改动就无效了。而且如果两条规则冲突了，防火墙会不会当场崩溃？也许就因为考虑到这些因素，至今没见过有多少产品提供过滤规则更新功能的，这并不能和杀毒软件的病毒特征库升级原理相提并论。

为了解决这种鱼与熊掌的问题，人们对包过滤技术进行了改进，这种改进后的技术称为动态包过滤。与它的前辈相比，动态包过滤功能在保持着原有静态包过滤技术和过滤规则的基础上，会对已经成功与计算机连接的报文传输进行跟踪，并且判断该连接发送的数据包是否会对系统构成威胁，一旦触发其判断机制，防火墙就会自动产生新的临时过滤规则或者对已经存在的过滤规则进行修改，从而阻止该有害数据的继续传输。但是由于动态包过滤需要消耗额外的资源和时间来提取数据包的内容进行判断处理，与静态包过滤相比，动态包过滤会降低运行效率，但是静态包过滤技术已经几乎退出市场了，能选择的，大部分也只有动态包过滤防火墙了。

2.2 应用代理技术

由于包过滤技术无法提供完善的数据保护措施，而且一些特殊的报文攻击仅仅使用过滤的方法并不能消除危害(如 SYN 攻击、ICMP 洪水等)，因此人们需要一种更全面的防火墙保护技术，在这样的需求背景下，采用应用代理技术的防火墙诞生了。代理服务器作为一个为用户保密或者作为突破访问限制的数据转发通道，在网络上应用广泛。一个完整的代理设备包含一个服务端和一个客户端，服务端接收来自用户的请求，调用自身的客户端模拟一个基于用户请求的连接到目标服务器，再把目标服务器返回的数据转发给用户，完成一次代理工作过程。应用代理防火墙，实际上就是一台小型的带有数据检测过滤功能的透明代理服务器，但是它并不是单纯地在一个代理设备中嵌入包过滤技术，而是嵌入一种被称为应用协议分析的新技术。

“应用协议分析”技术工作在 OSI 模型的最高层——应用层上，在这一层里能接触到的所有数据都是最终形式，也就是说，防火墙“看到”的数据和用户看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。

整个代理防火墙把自身映射为一条透明线路，在用户方面和外界线路看来，它们之间的连接并没有任何阻碍，但是这个连接的数据收发实际上是经过了代理防火墙转向的。当外界数据进入代理防火墙的客户端时，应用协议分析模块便根据应用层协议处理这个数据，通过预置的处理规则查询这个数据是否会产生危害，由于这一层面对的已经不再是组合有限的报文协议，所以防火墙不仅能根据数据层提供的信息判断数据，更能像管理员分析服务器日志那样看内容辨危害。而且由于工作在应用层，防火墙还可以实现双向限制，在过滤外部网络有害数据的同时也监控着内部网络的信息，管理员还可以配置防火墙实现身份验证和连接时限的功能，从而进一步防止内部网络信息的泄漏。

最后，由于代理防火墙采取的是代理机制进行工作，内外部网络之间的通信都需要先经过代理服务器审核，通过后再由代理服务器连接，根本没有给分隔在内外部网络两边的计算机直接会话的机会，因此可以避免入侵者使用“数据驱动”攻击方式(一种能通过包过滤技术防火墙规则的数据报文，当它进入计算机后，可变成能够修改系统设置和用户数据的恶意代码)渗透内部网络，可以说，应用代理技术比包过滤技术更完善。

但是，应用代理型防火墙的结构特征又偏偏是它最大的缺点。由于它是基于代理技术的，通过防火墙的每个连接都必须建立在为之创建的代理程序进程上，而代理进程自身是要消耗一定时间的，而且代理进程里还有一套复杂的协议分析机制在同时工作，于是数据在通过代理防火墙时就会不可避免地发生数据迟滞现象。通俗地讲，每个数据连接在经过代理防火墙时都会先被请进保安室喝杯茶搜搜身再继续赶路，而保安的工作速度并不能很快。代理防火墙是以牺牲速度为代价换取了比包过滤防火墙更高的安全性能的，在网络吞吐量不是很大的情况下，也许用户不会察觉到什么，然而到了数据交换频繁的时刻，代理防火墙就成了整个网络的瓶颈，而且一旦防火墙的硬件配置支撑不住高强度的数据流量而罢工，整个网络可能就会因此瘫痪了。目前，代理防火墙的普及范围远远不及包过滤型防火墙。

2.3 状态监视技术

状态监视技术是在包过滤技术和应用代理技术之后发展的防火墙技术。它是由自适应代理技术公司 CheckPoint 在基于包过滤原理的动态包过滤技术发展而来的，与之类似的有其他厂商联合发展的深度包检测技术。这种防火墙技术通过状态监视模块，在不影响网络安全正常工作的前提下采用抽取相关数据的方法对网络通信的各个层次进行监测，并根据各种过滤规则做出安全决策。

状态监视技术在保留了对每个数据包的头部、协议、地址、端口、类型等信息进行分析的基础上进一步发展了会话过滤(Session Filtering)功能，在每个连接建立时，防火墙会为这个连接构造一个会话状态，里面包含了这个连接数据包的所有信息，以后这个连接都基于这个状态信息进行。这种检测的高明之处是能对每个数据包的内容进行监视，一旦建立了一个会话状态，此后的数据传输都要以此会话状态作为依据。例如：一个连接的数据包源端口是 8000，那么在以后的数据传输过程里防火墙都会审核这个包的源端口还是不是8000，如果不是，这个数据包就被拦截，而且会话状态的保留是有时间限制的，在超时的范围内如果没有再进行数据传输，这个会话状态就会被丢弃。状态监视技术可以对数据包内容进行分析，从而摆脱了传统防火墙仅局限于检测几个包头部信息的弱点。而且这种防火墙不必开放过多端口，进一步杜绝了可能因为开放端口过多而带来的安全隐患。

由于状态监视技术相当于结合了包过滤技术和应用代理技术，因此是最先进的。但是由于实现技术复杂，状态监视技术在实际应用中还不能做到真正的完全有效的数据安全检测，而且在一般的计算机硬件系统上很难设计出基于此技术的完善防御措施。

课后习题二

一、选择题

1. 以下(　　)不是实现防火墙的主流技术。

A. 包过滤技术　　B. 应用级网关技术　　C. 代理服务器技术　　D. NAT 技术

2. 关于防火墙技术的描述中，正确的是(　　)。

A. 防火墙不能支持网络地址转换

B. 防火墙可以布置在企业内部网和 Internet 之间

C. 防火墙可以查、杀各种病毒

D. 防火墙可以过滤各种垃圾文件

3. 包过滤防火墙通过(　　)来确定数据包是否能通过。

A. 路由表　　B. ARP 表　　C. NAT 表　　D. 过滤规则

4. 以下关于防火墙技术的描述，(　　)是错误的。

A. 防火墙分为数据包过滤和应用网关两类

B. 防火墙可以控制外部用户对内部系统的访问

C. 防火墙可以阻止内部人员对外部的攻击

D. 防火墙可以分析和统管网络使用情况

5. 包过滤型防火墙工作在(　)。

A. 会话层　　B. 应用层　　C. 网络层　　D. 数据链路层

6. 公司的 Web 服务器受到来自某个 IP 地址的黑客反复攻击，你的主管要求你通过防火墙来阻止来自那个地址的所有连接，以保护 Web 服务器，那么你应该选择(　　)防火墙。

A. 包过滤型　　B. 应用级网关型　　C. 复合型防火墙　　D. 代理服务型

二、简答题

1. 请简述防火墙的工作原理。

2. 请简述包过滤防火墙的工作原理。

3. 请简述应用代理网关防火墙的工作原理。

第3章 防火墙的安全标准与评价体系

3.1 防火墙的安全标准

防火墙技术发展很快，但缺乏通用标准，导致各大防火墙产品供应商生产的防火墙产品兼容性差，给不同厂商的防火墙产品的互联带来了困难。为了解决这个问题，目前已提出了两个标准：

(1) RSA 数据安全公司与一些防火墙的生产厂商(如 Sun Microsystem 公司、Checkpoint 公司、TIS 公司等)以及一些 TCP/IP 协议开发商(如 FTP 公司等)提出了 Secure/WAN(S/WAN)标准，它能使在 IP 层上由支持数据加密技术的不同厂家生产的防火墙和 TCP/IP 协议具有互操作性，从而解决了建立虚拟专用网(VPN)的一个主要障碍。该标准包含两个部分：

① 防火墙中采用的信息加密技术一致，即加密算法、安全协议一致，使得遵循此标准生产的防火墙产品能够实现无缝互联，但又不失去加密功能。

② 安全控制策略的规范性、逻辑上的正确合理性，避免了各大防火墙厂商推出的防火墙产品由于安全策略上的漏洞而对整个内部保护网络产生危害。

(2) 美国国家计算机安全协会(National Computer Security Association，NCSA)成立的防火墙开发商(Firewall Product Developer，FWPD)联盟制订的防火墙测试标准。

3.2 防火墙的评价体系

防火墙是网络安全体系中最基础的保护环节，其重要性不言而喻。市场上有许多不同的防火墙，它们的体系结构和硬件参数各不相同，所服务的对象也不一样。那么用户应该如何选择呢？下面将介绍如何对防火墙进行评价。

1. 吞吐量

网络中的数据是由数据包组成的，防火墙对每个数据包的处理要耗费资源。吞吐量是指在没有帧丢失的情况下，设备能够接受的最大速率。其测试方法是：在测试中以一定速率发送一定数量的帧，并计算待测设备传输的帧，如果发送的帧数量与接收的帧数量相等，那么就将发送速率提高并重新测试；如果接收帧数量少于发送帧数量，则降低发送速率重新测试，直至得出最终结果。吞吐量测试结果以比特/秒或字节/秒表示。

吞吐量和报文转发率是关系防火墙应用的主要指标，一般采用 FDT(Full Duplex Throughput)来衡量，FDT 指 64 字节数据包的全双工吞吐量。该指标既包括吞吐量指标也涵盖了报文转发率指标。

随着 Internet 的日益普及，内部网用户访问 Internet 的需求在不断增加，一些企业也需