21世纪高等职业教育计算机系列规划教材

信息安全产品配置与应用

武春岭　主　编
李贺华　副主编

- 以防火墙、入侵检测等核心信息安全产品应用为载体，培养学生信息安全综合防御能力
- 采用项目导向、任务驱动，基于典型工作任务组织教学内容

配备电子教案

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

21 世纪高等职业教育计算机系列规划教材

信息安全产品配置与应用

武春岭　主　编
李贺华　副主编

高　林　主　审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书是一本专注于信息安全产品的教材，内容涵盖了防火墙、VPN、入侵检测、网络隔离、安全审计及上网行为管理、网络存储、数据备份、防病毒等常用信息安全设备，详细介绍了它们各自的功能、工作原理、配置，以及应用部署方案。

本书的写作融入了作者丰富的教学和工程实践经验，采用项目导向、任务驱动，基于典型工作任务组织教学内容，每个章节都专注于特定的主题，讲解通俗，案例丰富，力争让读者能够在最短的时间内掌握核心安全设备的基本操作与应用技能、快速入门与提高。

本书不仅可以作为高职、高专计算机信息类专业学生的教材，也可作为企事业单位网络信息系统管理人员的技术参考手册，尤其适合想在短期内快速掌握安全产品应用与部署的用户。

图书在版编目（CIP）数据

信息安全产品配置与应用 / 武春岭主编. —北京：电子工业出版社，2010.10
（21 世纪高等职业教育计算机系列规划教材）
ISBN 978-7-121-11868-5

Ⅰ.①信… Ⅱ.①武… Ⅲ.①信息系统－安全技术－高等学校：技术学校－教材 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2010）第 184561 号

策划编辑：徐建军
责任编辑：徐建军　　特约编辑：李云霞
印　　刷：涿州市京南印刷厂
装　　订：涿州市桃园装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：18　字数：460.8 千字
印　　次：2010 年 10 月第 1 次印刷
印　　数：3 000 册　　定价：29.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着互联网在中国的快速发展与普及，人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化。互联网在促进经济结构调整、经济发展方式转变等方面发挥着越来越重要的作用，目前中国已成为世界上互联网使用人口最多的国家。然而，互联网安全问题日益突出，成为各国普遍关切的问题，中国也面临着严重的网络安全威胁。

近几年来，随着网络技术的迅速发展，网络环境也更加复杂化。计算机网络安全威胁的日益严重，如病毒和蠕虫不断扩散、黑客活动频繁、垃圾邮件猛增等都成为目前困扰网络信息安全的较大网络威胁。比如，2009 年新的安全威胁 Conficker（飞客）的出现，打破了全球 500 万台计算机的感染记录，这些都迫使计算机用户不断地提高防范意识，并对信息安全产品提出了更高需求。

目前，信息安全最基本的防护手段是构建完善的信息安全防御平台，以防火墙、入侵检测产品为代表的信息安全产品构建综合防御体系，构建保障信息安全的基础屏障。信息安全产品已经成为政府、金融和其他企事业单位信息化推进的基本硬件保障，市场对信息安全产品的需求日益增长。与此同时，信息安全厂商、信息系统集成商和信息系统运营商对信息安全产品技术支持和技术服务的专业人员需求也与日俱增、日趋迫切。

重庆电子工程职业学院信息安全技术专业，是国家示范院校建设中唯一一个信息安全类国家级重点建设专业，该专业自 2003 年开办以来，就开设了“信息安全产品配置与应用”课程，目前该课程已经获得重庆市市级精品课程称号。我们根据多年的教学实践，与天融信公司合作，编写了该专业的核心技术教材，旨在更有效地培养信息安全产品工程师（产品销售工程师、产品维护工程师和产品技术支持工程师）。

作为一本专注于信息安全产品的教材，本书详细介绍了信息安全领域常用产品的配置与应用及产品部署方案。本书共 8 章，第 1 章讲述防火墙产品配置与应用；第 2 章讲述 VPN 产品配置与应用；第 3 章讲述入侵检测产品配置与应用；第 4 章讲述网络隔离产品配置与应用；第 5 章讲述安全审计及上网行为管理产品配置与应用；第 6 章讲述网络存储设备配置与应用；第 7 章讲述数据备份软件配置与应用；第 8 章讲述防病毒过滤网关系统配置与应用。

本书的写作融入了作者丰富的教学和企业实践经验，内容安排合理，每个章节都专注于特定主题，讲解通俗，案例丰富，力争让读者能够在最短的时间内掌握核心安全设备的基本操作与应用技巧、快速入门与提高。本书第 1 章、第 5 章和第 8 章由武春岭编写，第 2 章由路亚编写，第 3 章、第 4 章由鲁先志编写，第 6 章、第 7 章由李贺华编写。

为了方便教师教学，本书配有电子教学课件，有此需要的教师可登录华信教育资源网（www.hxedu.com.cn）免费注册后进行下载，有问题时可在网站留言板留言或与电子工业出版社联系（E-mail：hxedu@phei.com.cn）。

本书在编写过程中，得到了教育部高等学校高职高专电子信息类专业教学指导委员会高林主任、鲍洁秘书长和盛鸿宇秘书的指导。此外，天融信公司成都分公司周非副总经理和魏振国工程师的大力支持和帮助，在此一并致以衷心的感谢！

由于编者水平有限，加上时间仓促，书中难免有不当之处，敬请各位同行与读者批评指正，以便在今后的修订中不断改进。

编　者

反侵权盗版声明

目　录

第 1 章　防火墙产品配置与应用

学习目标

- 了解防火墙基本技术及发展历史。
- 了解防火墙工作原理及关键技术。
- 掌握防火墙系统部署方式。
- 掌握防火墙应用方案及安全策略的设计方法。
- 掌握天融信防火墙基本配置方法。

引导案例

某集团公司，随着业务的发展对信息化的依赖逐渐提高，信息化的高效率也为该集团的快速发展提供了有力的保障。企业的核心系统如 OA、ERP、财务系统等均已实现网络应用、异地互连的状态，可以让员工随时随地访问，极大地提升了办公效率。以前需要跑来跑去几天才能完成的纸质文件办公方式，现在 1 个小时就可以圆满完成。

然而，该集团虽然很注重自身信息化平台的建设，但却忽略了网络安全，集团核心网使用了各种高档交换、路由设备，但没有部署包括防火墙在内的任何网络安全产品。因为接入了互联网，企业的核心应用系统在 2009 年被黑客入侵，后来经过专业公司的调查，发现这个有心计的黑客其实早已入侵该集团网络，一直处于潜伏窃取集团资料的状态，在该集团的一次商业竞标中，才发现竞争对手竟然已经非常了解自己的投标机密。

于是，该集团公司第一次意识到了问题的严重性，随后集团聘请了专业的网络安全技术公司，对该集团的网络、信息资产、业务等内容进行了全面的风险评估，并提出了包括使用防火墙、VPN、入侵防御等技术手段来提高该集团的网络安全级别。该集团于 2009 年年底，完成了一期的网络安全建设，在集团总部及下属数十家单位的互联网出口，全面部署了防火墙系统，通过防火墙系统实现了对集团总部及其下属单位与互联网之间的访问控制，极大地提升了抵御互联网攻击、入侵的能力，同时通过防火墙系统的部署，实现了对网络应用办公流量的控制，提升了集团互联网办公带宽的利用效率。根据防火墙的日志记录，自一期项目完成后，防火墙已经成功抵御过数次来自互联网针对该集团应用系统的攻击入侵行为。

……

2010 年年初，某政府行业用户，在某区域 40 余个区县，完成了 50 余台防火墙设备的部署，实现了对这 50 余个直属单位网络的安全访问控制，提升了其网络的整体安全性。使其日常办公应用的安全性与稳定性得到了全面提升。

2009 年年底，某国防单位，在全国范围内实施了一次网络边界防护项目，在该单位专网上，为每个接入点接入边界部署了一套防火墙系统，使每个接入点在访问总部或被其他节点访问时的网络流量均能被部署的防火墙系统进行检测和控制，极大地提升了整体网络及节点网络

的安全性，其应用系统因违规网络流量带来的故障率由原来的5%直线降低到0.5%。

2009年年初，某大型企业，为提高企业网络使用效率、降低网络病毒感染率及遭受网络攻击的可能性，在企业互联网边界及内部服务器区域边界，部署了多功能防火墙系统，系统部署后大大地降低了网管人员的日常工作强度，全面提升了互联网带宽的利用效率，在潜移默化中为企业带来了无形的价值收入。

……

防火墙（Firewall）系统作为采用访问控制过滤技术的代表产品已经被越来越多的用户认可，其作为网络安全最基本、经济、有效的手段之一，通常部署在内、外两个网络（或多个网络）或者两个网络安全域的边界处，对经过防火墙系统的数据进行检测、判断是否符合制定的通信策略，决定是否进行数据转发，有效地对内、外网络实施隔离，严格保护内部网络不受非授权信息的入侵和访问。防火墙可以实现内、外网或不同信任域之间的网络隔离与访问控制。同时，它也是任何一个网络安全建设必不可少的安全产品。据有关数据统计，防火墙的建设会使整个网络的安全风险降低90%。

在最近10年的用户信息安全项目调研中发现，不管是政府、企业还是金融、军队等，各个行业在自己的网络安全建设中，均将防火墙的部署作为网络安全建设的第一步，可见防火墙在实际应用中的意义之大。为能让大家全面地了解防火墙技术、产品及其技术发展状况，本章将对防火墙进行全面的介绍，配合实际操作让大家加深印象，并达到可以独立完成防火墙产品部署方案设计及产品实际部署配置的目的。

相关知识

1.1　防火墙概述

1.1.1　什么是防火墙

防火墙原是建在大楼内用于防火的一道墙，就如森林里的隔离带或防止外敌入侵的护城河。在计算机网络中，防火墙是设置在被保护网络和外部网络之间的一道屏障，以防止发生不可预测的、潜在的破坏性入侵，保护网络内部的安全。

防火墙是不同网络（如可信任的企业内部网和不可信任的公共网）或网络安全域之间信息的唯一出入口，本身具有强大的抗攻击能力，可以根据企业的安全政策（允许、拒绝、监测）控制出入网络的信息流。

物理上，防火墙是设置在不同网络或网络安全域之间的一系列部件的组合。逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器。

1.1.2　防火墙的功能

1. 防火墙是网络安全的屏障

防火墙通过过滤不安全的服务降低风险，能够极大地提高内部网络的安全性。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。比如，防火墙可以禁止众所周知的不安全的NFS协议进出受保护的网络，这样外部的攻击者就不可能利用这

些协议的脆弱性来攻击内部网络。防火墙还可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。

2．防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如，在网络访问时，一次口令系统和其他的身份认证系统完全不必分散在各个主机上，而是集中在防火墙上。

3．对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的，可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4．防止内部信息的外泄

利用防火墙对内部网络的划分，可实现内部网络中重点网段的隔离，从而限制局部重点或敏感网络安全问题对全局网络造成的影响。隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节的（如 Finger、DNS 等）服务。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等，而且 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意，等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布于世界各地的 LAN 或专用子网有机地连成一个整体，不仅省去了专用通信线路，而且为信息共享提供了技术保障。

1.1.3　防火墙的局限性

1．限制有用的网络服务

防火墙为了提高被保护网络的安全性，限制或关闭了很多有用但存在安全缺陷的网络系统服务。由于绝大多数网络服务在设计之初根本没有考虑安全性，只考虑使用的方便和资源共享，所以难免存在安全问题。这样防火墙将限制这些服务，等于从一个极端走到了另一个极端。

2．无法防止内部网络用户的攻击

目前，防火墙只是提供对外部网络用户的防护，对来自内部网络用户的攻击只能依靠

网络主机系统的安全性。也就是说，防火墙对内部网络用户来讲形同虚设，目前还没有更好的解决办法，只有采用多层防火墙系统。

3．无法防范不经过防火墙的攻击

假如，在一个被保护的网络上有一个没有限制的拨出存在，内部网络上的用户就可以直接通过 SLIP 或 PPP 连接进入 Internet。用户可能会对需要附认证的代理服务器感到厌烦，因而向 ISP（互联网服务提供商）或 ISP 连接，从而试图绕过由精心构造的防火墙提供的安全系统。这就为从后门攻击创造了极大的可能。网络用户必须了解这种类型的连接对于一个有安全保护系统来说是绝对不允许的。

4．不能完全防止传送已感染病毒的文件

因为病毒的类型太多，操作系统也有多种，编码与压缩二进制文件的方法也各不相同。所以不能期望 Internet 防火墙对每一个文件进行扫描，查出潜在的病毒。对病毒特别关心的机构应在每个桌面部署防病毒软件，防止病毒从软盘或其他来源进入网络系统。

5．无法防范数据驱动型的攻击

数据驱动型的攻击从表面上看是无害的数据被邮寄或复制到 Internet 主机上，但一旦执行就开始攻击。例如，一个数据型攻击可能导致主机修改与安全相关的文件，使得入侵者很容易获得对系统的访问权。后面章节中我们将会看到，在堡垒主机上部署代理服务器是禁止从外部直接产生网络连接的最佳方式，并能减少数据驱动型攻击的威胁。

6．不能防备新的网络安全问题

防火墙是一种被动式的防护手段，只能对已知的网络威胁起作用。随着网络攻击手段的不断更新和一些新的网络应用的出现，不可能靠一次性的防火墙设置来解决永久的网络安全问题。

1.2　防火墙的体系结构

1.2.1　防火墙系统的构成

防火墙由一个或多个构件组成，这些构件有：

- 包过滤型路由器；
- 应用层网关（或代理服务器）。

根据构成，现有的防火墙主要分为包过滤型、代理服务器型、复合型，以及其他类型。包过滤型防火墙通常安装在路由器上，大多数路由器都提供了包过滤的功能。包过滤在网络层进行，以 IP 包信息为基础，对 IP 源地址、目标地址、协议类型、端口号等进行筛选。代理服务器型防火墙通常由两部分构成，即服务器端程序和客户端程序。客户端程序与中间节点连接，中间节点再与提供服务的服务器实际连接。复合型防火墙将包过滤和代理服务两种方法结合起来，形成新的防火墙，由堡垒主机提供代理服务。

1．包过滤型路由器

包过滤型路由器对所接收的每个数据包做允许或拒绝的决定。路由器审查每个数据报以便确定其是否与某一条包过滤规则相匹配。过滤规则基于可以提供给 IP 转发过程的包头信息。包头信息中包括 IP 源地址、IP 目标端地址、封装协议（ICP、UDP、ICMP 或 IP Tunnel）、TCP/UDP 目标端口、ICMP 消息类型、包的进入接口和输出接口。如果可以匹配并且规则允许该数据包，那么该数据包就会按照路由表中的信息被转发。如果匹配但是规则拒绝该数据包，那么该数据包就会被丢弃。如果没有相匹配的规则，用户配置的默认参数会决定是转发还是丢弃数据包。

1）与服务相关的过滤

包过滤型路由器使得路由器能够根据特定的服务允许或拒绝流动的数据，因为多数的服务提供者都在已知的 TCP/UDP 端口号上监听请求包的到来。例如，Telnet 服务器进程监听在 TCP 的 23 号端口，SMTP 服务器进程监听在 TCP 的 25 号端口。为了阻塞所有进入的 Telnet 连接，路由器只需简单地丢弃所有 TCP 端口号等于 23 的数据包即可。为了将进来的 Telnet 连接限制到内部的数台机器上，路由器必须拒绝所有 TCP 端口号等于 23 并且目标 IP 地址不等于允许主机的 IP 地址的数据包。

一些常用的典型包过滤规则包括：允许进入的 Telnet 会话与指定的内部主机连接；允许进入的 FTP 会话与指定的内部主机连接；允许所有外出的 Telnet 会话；允许所有外出的 FTP 会话；拒绝所有来自特定的外部主机的数据包；等等。

2）与服务无关的过滤

有几种类型的攻击很难使用基本的包头信息来识别，因为这几种攻击是与服务无关的。它们很难被指定，因为过滤规则需要附加的信息只能通过审查路由表和特定的 IP 选项，或检查特定段的内容等才能得到。但是，可以对路由器进行配置，以防止这几种类型的攻击。下面是这几种攻击类型的例子：

- 源 IP 地址欺骗式攻击（Source IP Address Spoofing Attacks）

源 IP 地址欺骗式攻击的特点是入侵者从外部传输一个假装是来自内部主机的数据包，即数据包中所包含的 IP 地址为内部网络上的 IP 地址。入侵者希望借助于一个假的源 IP 地址渗透到一个只使用了源地址安全功能的系统中。在这样的系统中，来自内部信任主机的数据包被接受，而来自其他主机的数据包全部被丢弃。对于源 IP 地址欺骗式攻击，可以利用丢弃所有来自路由器外部端口的使用内部源地址的数据包的方法来挫败。

- 源路由攻击（Source Rowing Attacks）

源路由攻击的特点是源站点指定了数据包在 Internet 中所走的路线。这种类型的攻击是为了旁路安全措施并导致数据包循着一个对方不可预料的路径到达目的地。只需简单地丢弃所有包含源路由选项的数据包即可防范这种类型的攻击。

- 极小数据段式攻击（Tiny Fragment Attacks）

极小数据段式攻击的特点是入侵者使用了 IP 分段的特性，创建极小的分段并强行将 TCP 包头信息分成多个数据包段。这种攻击是为了绕过用户定义的过滤规则。黑客寄希望于过滤器路由器只检查第一个分段而允许其余的分段通过。对于这种类型的攻击，只要丢弃协议类型为 TCP、IP Fragment Offset 等于 1 的数据包就可安然无恙。