THOMSON

# GUIDE TO FIREWALLS AND NETWORK SECURITY

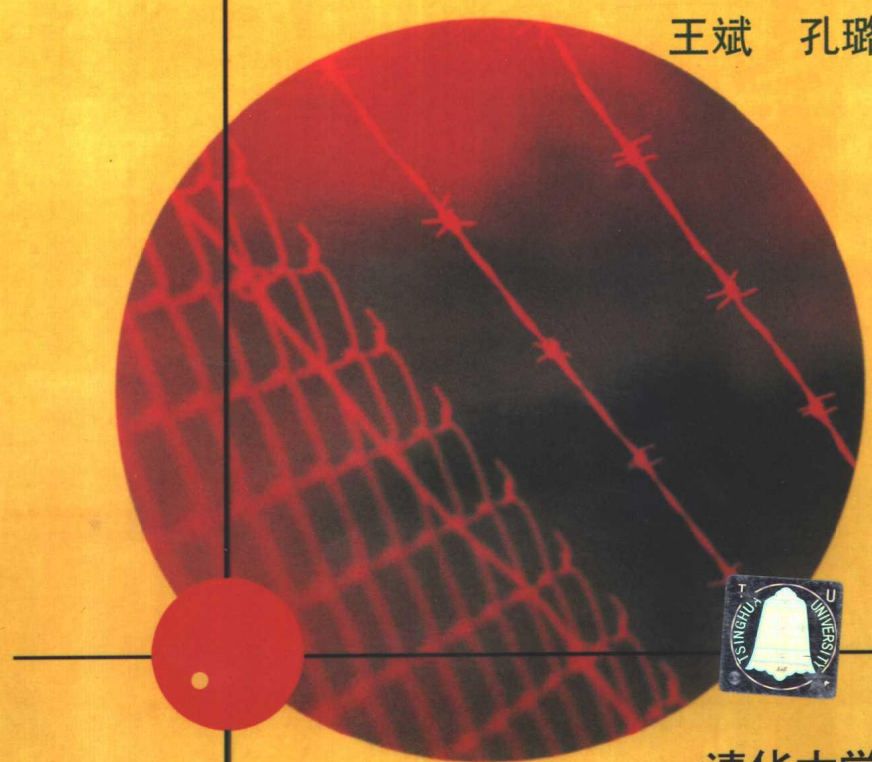
## INTRUSION DETECTION AND VPNs

# 防火墙与网络安全

## ——入侵检测和 VPNs

(美) Greg Holden 著

王斌 孔璐 译



清华大学出版社

# 防火墙与网络安全

## ——入侵检测和 VPNs

(美) Greg Holden 著

王斌 孔璐 译

清华大学出版社

北 京

EISBN: 0-619-13039-3



981-254-540-9

北京市版权局著作权合同登记号　图字：01-2003-3438

**本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。**

**图书在版编目(CIP)数据**

防火墙与网络安全——入侵检测和 VPNs/(美)侯登(Holden, G.)著；王斌，孔璐译.—北京：清华大学出版社，2004

书名原文：Guide to Firewalls and Network Security: Intrusion Detection and VPNs

ISBN 7-302-08572-2

Ⅰ. 防…　Ⅱ. ①侯…②王…③孔…　Ⅲ. 计算机网络—防火墙　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2004)和 039175 号

出 版 者：清华大学出版社　　地　　址：北京清华大学学研大厦
http://www.tup.com.cn　　邮　　编：100084
社 总 机：010-62770175　　客户服务：010-62776969

组稿编辑：曹康
文稿编辑：李阳
封面设计：康博
版式设计：康博
印 刷 者：北京昌平环球印刷厂
装 订 者：北京市密云县京文制本装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　印张：20.5　字数：524 千字
版　　次：2004 年 6 月第 1 版　2004 年 6 月第1 次印刷
书　　号：ISBN 7-302-08572-2/TP·6149
印　　数：1～4000
定　　价：40.00 元

# 前　言

本书旨在介绍防火墙和其他网络安全组件，将它们组合起来可以创建 LAN 周围的深层防御边界。如今，防火墙是使用得最为广泛的安全工具，它们在一般用户及信息技术专家中正日益普及。然而，如果获得安全策略的支持，并能与反病毒软件、入侵检测系统和其他工具结合起来使用，防火墙的作用将得到最大程度的发挥。

同时，本书还将防火墙与有效的边界安全及网络安全性所需要的其他因素结合起来讨论。这些因素包括包过滤、身份验证、代理服务器、加密、堡垒主机、虚拟专用网络(VPN)、日志文件维护和入侵检测系统等。

## 本书主要内容

让读者无需从头至尾按顺序阅读本书。然而，前三章对防火墙及其适合于网络安全程序之处作了全面介绍，因此强烈建议您从这三章开始阅读。其内容如下所示：

第 1 章“防火墙规划和设计”概述了各种不同的防火墙和它们的主要功能，这样您可从中选择满足需要的合适的防火墙。

第 2 章“开发安全策略”帮助您协调防火墙目标和组织的整体安全策略的目标。您还会学到如何一步一步地与管理部门一起工作，确保安全策略奏效。

第 3 章“防火墙配置策略”介绍了将一个或多个防火墙定位到网络边界，并协调它们与其他组件(如 DMZ、路由器和 VPN)一起工作的不同方法。

接下来的一些章节讨论了对于防火墙和网络安全来说比较重要的特定主题。您会发现这几章对您有最直接的意义，而不是流于形式。第 4 章“数据包过滤”讨论了最初始的，有时也是最基本的防火墙活动，介绍了无状态和有状态的包过滤，以及如何针对通用的协议(例如 ICMP、TCP 和 UDP)建立规则集。第 5 章“代理服务器和应用级防火墙”讨论了代理服务器如何代表网络上的单台主机工作，以对它们提供保护。第 6 章“用户身份验证”描述了防火墙进行身份验证的原因，它们如何通过用户、客户端和会话验证，以及集中式身份验证和一次性口令系统来确认经过授权的个体。第 7 章“加密和防火墙”重点是防火墙体系结构中的角色加密和为网络建立 PKI。第 8 章“选择堡垒主机”解释了如何保护运行有防火墙、入侵检测软件或是在 DMZ 上提供公共服务的主机的安全。

本书的最后三章深入讨论了一些高级主题，重点考虑了流行的防火墙和 VPN 选项。第 9 章“创建虚拟专用网”讨论了 VPN 的建立，它为公司提供了在公共 Internet 进行安全通信的经济可行的方法。因为 VPN 使用加密和身份验证，在阅读本章之前先阅读第 6 章和第 7 章将很有好处。第 10 章“建立自己的防火墙”向您讲述了两类防火墙，解释了桌面防火墙和企业防火墙

如何工作。第 11 章“防火墙管理”讨论了在管理防火墙时需要定期执行的不同维护任务，包括日志文件轮循和检查。本章还深入介绍了反病毒软件和入侵检测系统与防火墙的整合。

读者还将被指导查看一些在线资源以及本书提到的一些印刷品。

## 本书特色

为了帮助您全面了解网络概念，本书提供了许多有特色的内容，以便提升其教学价值。

- **本章学习目标**：本书每章的开头都列出了本章中应掌握的一些概念。这一列表可以使您很快地了解到该章的主要内容，可以对学习起到帮助作用。
- **示意图表和截图**：大量的网络配置图解可以帮助您直观地了解防火墙的常规设置和体系结构。另外，大量的例表用理论和实际的数据提供了详细的内容和比较。有些表提供了用于构建防火墙规则集的包过滤规则的具体示例。因为大部分学校实验室使用 Microsoft 操作系统，所以本书的图及实用项目都采用 Microsoft 操作系统的产品。
- **本章小结**：每章的最后都会对这章的内容作个总结。这些小结为重述和回顾每章所讲的内容提供了有用的参考。
- **关键术语**：在本章小结后面，列出了一些新的网络术语和它们的定义，这可以帮助正确理解每章的主要概念，并提供有用的参考。
- **复习题**：每章后面都提供了一组复习题，以巩固每章中的学习要点。这些问题可确保您真正掌握这些概念。
- **实用项目**：尽管理解网络技术背后的原理很重要，但只有通过实践才能得到提高。除了纯理论的东西外，每章还提供了一系列用于给学生们提供实践经验的练习。
- **案例项目**：最后，每章结尾都提供一些特定的与防火墙和与安全相关的建议方案。您被要求评估这些情况，决定该采取的行动来弥补所描述的问题。该部分内容将帮助您提高迅速作出决定和除错的技能——这种技能是防火墙和安全系统管理的一个重要方面。

## 附录和术语表

除了这些外，本书还包括下列内容：

- 附录 A：安全性资源：附录提供了一些可在线找到的与安全相关的最新信息的站点。您可以获得一些知名站点提供的信息，关于网络安全及病毒警告的背景知识，并可以测试已有网络配置的端口扫描器，以及可帮助您找到用于网络安全领域的证书的地方。
- 术语表：这是本书中使用的所有缩略词和技术术语的总目录，包括其定义。

## 顺应 Web 的改变

总有一天，本书附录提到的所有基于 Web 的资源都会过时，或是被更新的资源所淘汰。在有些情况下，您从本书所了解到的 URL 将把您带到它们的替代品那儿，而另外的情况则是，显

示令人讨厌的 404 错误消息："File not found。"

如果发生这种情况，请不要放弃！如果您愿意花些时间和精力，通常通过 Web 都可以找到您想要的信息。而许多大型、综合性的 Web 站点都提供了搜索引擎。只要访问这些站点，您就可以使用这一工具帮助您找到所需的。

不要对使用 http://www.google.com、http://www.hotbot.com 或 http://www.excite.com 这样的搜索工具来搜索相关信息感到害怕。一些标准组织可能在线提供了有关他们的标准的、最准确的特定信息，此外还存在大量第三方的关于在这一领域的练习和帮助。如果无法找到书中所指示的内容，可以去别处找找。

## Web 资源

可从网络上找到特别为本书设计的一些附加资源。请访问 www.course.com，定期搜索本书主题，可获得详细的内容。

## 阅读准备

本书包括了 70 多个实用项目，其中大部分都要求您安装和使用不同的与安全性相关的软件。您需要一台与 Internet 相连的计算机，在该计算机上应可以运行这些程序。推荐使用的软硬件如下所示。

- **硬件要求**

计算机的 CPU 必须至少为奔腾 II，运行速度为 300MHz 或更快。要能够同时运行 Web 浏览器、字处理程序以及其他程序，至少需要 192MB 的 RAM(理想的大小是 256MB 或是更高)和最少 75MB 的可用磁盘空间。

- **软件要求**

本书中的大部分项目可使用运行 Windows 2000/XP 或 Red Hat Linux 7.3 或更高版本的计算机完成。

实用项目中使用的大部分程序要求您下载和安装相关软件。至少，您的计算机需要安装 Web 浏览器和压缩程序 WinZip(可从 www.winzip.com 中获得)。还需要一个字处理程序或文本编辑器，用以记录从实用项目中获得的结果。在有些项目中，还需要用到电子邮件程序，例如 Outlook Express 或 Netscape Messager。

- **特殊要求**

在本书中，您将找到一些关于 Check Point NG 的参考。如果您有此软件，您的系统将需要至少 128MB 的 RAM 来运行它。注意，Check Point NG 运行于 Windows 2000 上；如果在 Windows XP 上运行，其功能将受到限制。

各章需要的可免费下载软件如下：

第 3 章：Syagte 个人防火墙，www.sygate.com

第 4 章：Tiny 个人防火墙，www.tinysoftware.com

第 5 章：NetProxy，www.grok.co.uk；SOCKS，www.socks.nec.com

第 7 章：PGP(Pretty Good Privacy)，http://web.mit.edu/network/pgp.html

第 8 章：NetScan Tool 4，www.netscantools.com；IP Sentry，www.ipsentry.com

第 9 章：Symantec Enterprise Virtual Private Network 7.0，www.symantec.com/downloads

第 10 章：ZoneAlarm Pro，www.zonelabs.com

**注意：**

在第 10 章，您将学习到 Linksys(www.linksys.com)，它提供了大量路由器、集线器、无线接入点、防火墙和其他硬件。该章中关于 Linksys 产品的引用和描述已经过 Linksys 允许。

# 目　　录

# 第1章　防火墙规划与设计

**本章学习目标：**

- 了解关于防火墙的一些误解
- 认识到防火墙基于一个有效的安全策略
- 理解防火墙的作用
- 描述防火墙提供的各种类型的保护
- 了解防火墙的各种限制
- 确定对防火墙硬件和软件的最优化配置

网络安全性由一系列不断发展的技术组成，特别应用在与通信或者商务服务的 Internet 相连接的网络中。网络安全性中近来最重要的一个发展就是，防火墙已作为了一个重要角色。由于黑客与恐怖分子的公开攻击、病毒和其他入侵软件的蔓延，防火墙已经成为一个基本的安全工具。防火墙现在实质上已不是每个网络以及许多个人计算机可有可无的部分，而是必需的产口。

没有一个安全系统能绝对保证它的信息一直都受到了保护。但是由于防火墙与安全策略配合使用，根据其保护的业务的需求进行开发，经常进行维护和升级，所以它是网络管理员可以部署的最有效的安全工具之一。

本章向您提供了在规划和设计防火墙方面所涉及诸多问题的大致介绍。首先，介绍一些关于防火墙的错误理解——“防火墙 101 ”，以便于您一开始就可以对防火墙的概念有一个更加清晰的认识。接下来学习用以控制防火墙工作的一些安全策略、标准以及程序。然后学习防火墙保护的类型、防火墙的限制以及如何利用硬件创建防火墙。本章最后对防火墙软件包进行了评价。

**注意：**

*在本书中，“防火墙”这一术语并不一定表示防火墙只是一个路由器、计算机、VPN 网关或者软件程序。任何单独的防火墙程序实际上是由若干软件和硬件组件组合而成的。*

在本章中，我们假定您对 TCP/TP 和网络基础设施的有基础的了解。同时假定您了解 IP 地址和域系统等内容，并熟悉 Internt 和基于 Web 的软件。如果在阅读完本章后，您对 TCP/TP 或网络基础设施其他方面的基础知识有些不解的话，可以通过访问 www.course.com 来提高您的技能。

## 1.1　关于防火墙的误解

许多人都曾听说过“防火墙”这个术语，但是并没有把它与 Internet 联系起来。他们可能曾经听过他们的汽车技工提到过在汽车内部和发动机之间存在着一道防火屏障，或许将之理解成