计算机安全技术丛书

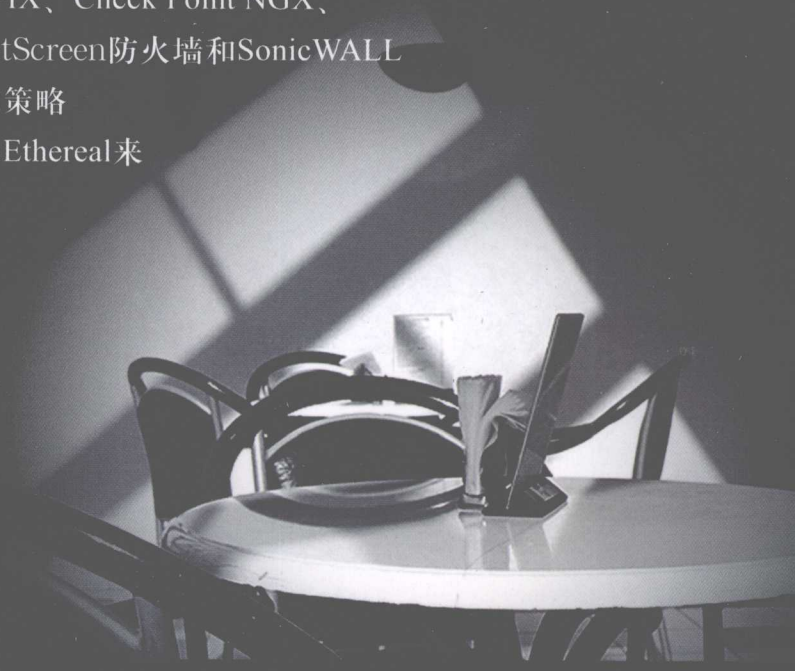
防火墙策略与VPN配置

[美] Mark Lucas　Abhishek Singh　Chris Cantrell　编著

谢　琳　赵　俐　黄铝文　译

多任务安全专家的基本实战指南

- 介绍市场上领先的防火墙：Cisco PIX、Check Point NGX、Microsoft ISA Server、Juniper的NetScreen防火墙和SonicWALL
- 重点关注创建可应用于多种产品的策略
- 附带介绍使用最流行的协议分析器Ethereal来监视和分析网络流量



中国水利水电出版社
www.waterpub.com.cn

计算机安全技术丛书

防火墙策略与 VPN 配置

Mark Lucas

[美] Abhishek Singh 编著

Chris Cantrell

谢 琳 赵 俐 黄铝文 译

中国水利水电出版社

内 容 提 要

本书是一本介绍防火墙和 VPN 概念及实施的实战指南。全书从概念出发，在对当前市场上领先的各类防火墙和 VPN 产品进行较为全面的比较分析的基础上，结合典型案例分析，深入阐述如何制定适合组织需要的安全策略及设计和实施防火墙与 VPN 解决方案。

全书共分为四部分：第一部分介绍网络安全策略；第二部分介绍防火墙的概念和实施；第三部分介绍 VPN 的概念以及如何选择 VPN；第四部分结合实例介绍不同规模的组织如何设计和实施防火墙和 VPN。

本书通俗易懂，实例丰富，既可作为网络安全专业人士的实战指南，也适合各类关注网络安全的人士参考。

北京市版权局著作权合同登记号：图字 01-2006-7280

图书在版编目（CIP）数据

防火墙策略与 VPN 配置 /（美）卢卡斯（Lucas,M.）等编著；谢琳等译. —北京：中国水利水电出版社，2008
（计算机安全技术丛书）
书名原文：Firewall Policies and VPN Configurations
ISBN 978-7-5084-5025-4
（计算机安全技术丛书）

Ⅰ. 防… Ⅱ. ①卢…②谢… Ⅲ. 计算机网络－安全技术
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 155137 号

书　　名	防火墙策略与 VPN 配置
作　　者	[美]Mark Lucas　Abhishek Singh　Chris Cantrell　编著
译　　者	谢　琳　赵　俐　黄铝文　译
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm　16 开本　23.25 印张　454 千字
版　　次	2008 年 1 月第 1 版　2008 年 1 月第 1 次印刷
印　　数	0001—4000 册
定　　价	45.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

译者序

防火墙和VPN是当今应用最为广泛的网络安全产品和技术，但是目前市场上的防火墙和VPN产品众多，最新一代防火墙的功能更可以说是令人眼花缭乱，而各类企业和组织的情况千差万别，如何才能在市场上众多品牌和型号的产品中选择最适合自身需求的产品，并且在实施过程中还能够充分发挥所选择产品的效用呢？其关键在于选择合适的产品和技术，并且编写精炼准确的安全策略，以便在安全和可用性之间寻求一个最佳平衡点。

本书从基本概念出发，结合典型案例，深入浅出地介绍了如何根据不同组织的需求来设计和实施防火墙和VPN。本书还对当前业界领先的各类防火墙产品进行了较为全面的分析比较，采用简单明了的文字介绍了这些产品的特性、弱点和复杂性，同时还对VPN策略进行了深入阐述。此外，本书还针对不同章节的主题提供了丰富的、极富价值的参考链接。

全书分为四部分：第一部分介绍网络安全策略的基本概念，本着编写与厂商无关策略的出发点，该部分介绍了如何定义通用的安全策略以及根据所编制的安全策略建立防火墙和VPN配置的基本原则。第二部分介绍防火墙，在介绍应用程序代理和网关等不同类型防火墙及其特点的基础上，重点分析比较了市场上常见的几种软硬件防火墙产品的特性，并由此阐述如何选择合适的防火墙解决方案。第三部分介绍VPN，在介绍什么是VPN并对业界流行的IPSec、SSL、SSH Tunnel和L2TP等VPN技术的特性和优缺点进行分析比较的基础上，本部分深入介绍了软、硬件VPN设备的特性，并对业界流行的各类产品进行了较为全面的比较分析，以便于读者进行选择。第四部分在介绍企业安全技术之根本的IT基础架构安全计划及其实施原则的基础上，通过两个典型规模的企业实例，介绍了如何结合各自的实际需求与情况，设计并采用不同的防火墙和VPN实施方案以保证企业安全。

本书由谢琳、赵俐、黄铝文翻译，在翻译过程中，得到了易磊、张猛、张波、欧阳宇、盛海燕、安晓梅、徐红霞的帮助，其中易磊审校了全文，在此一并致谢。由于时间仓促，加之译者水平有限，译文中错漏之处难免，敬请读者指正。

译者

2007年6月

关于作者

Mark J. Lucas（MCSE 和 GIAC 认证的 Windows 安全管理员）是加利福尼亚技术学院的高级系统管理员。Mark 负责各种高可用系统（如 Microsoft Exchange Server、运行在 VMWare ESX 之上的服务器和各种许可服务器）的设计、实现和安全。他还负责运用防火墙来保护这些系统。Mark 拥有 10 年的 IT 工作经验。这是 Mark 第一次为 Syngress 出版社著书。Mark 与其妻子 Beth，以及有“4 条腿的、毛茸茸的”孩子们 Aldo、Cali、Chuey 和 Emma 一起住在加利福尼亚的 Tujunga。

Chris Cantrell 是 Riverbed Technology 公司的售前系统工程师，该公司是广域网数据服务（Wide-area Data Service，WDS）市场的先锋。在加入 Riverbed 之前，Chris 花了 8 年时间专门研究网络安全和入侵防护，他在 Network Associates、OneSecure、NetScreen 和 Juniper Networks 等公司担任过不同的管理和工程技术职务。Chris 是 *Configuration NetScreen Firewall*（ISBN: 1-93226-639-9）一书的作者之一，该书由 Syngress 出版社于 2004 年出版。

Chris 和可爱且支持他的妻子 Maria 以及两个孩子 Dylan 和 Nikki 一起住在科罗拉多州的丹佛市。

Laura E. Hunter（CISSP、MCSE：Security、MCDBA、Microsoft MVP）是宾西法尼亚大学的 IT 项目负责人和系统经理，在那里她为大学内不同单位和学院提供网络规划、实现并负责故障排除。她的专长包括 Windows 2000 和 Windows 2003 Active Directory 的设计和实现、故障排除和安全。Laura 拥有超过 10 年使用 Windows 的计算机经验，她曾担任过 Salvation Army 的计算机服务主管、药物供应公司的 LAN 管理员。她还是 TechTarget 系列 Web 站点和 Redmond Magazine（以前称为 Microsoft Certified Professional Magazine）的撰稿人。

Laura 之前曾参与过 Syngress 的 *Windows Server 2003 MCSE/MCSA DVD Guide & Training System* 系列丛书的编写工作，她担任过该丛书的 DVD 设计者、作者和技术审校，而且还是 APress 的 *Active Directory Consultant's Field Guide*（ISBN: 1-59059-492-4）一书的作者。Laura 三次获得在 Windows 服务器连网领域颇有声望的 Microsoft MVP 奖项。Laura 是滨西法尼亚大学的荣誉毕业生，并且还是一名自由作家、培训讲师、演讲者和顾问。

Abhishek Singh 是 Third Brigade 公司的安全研究员，这是一家位于加拿大的信息安全公司。他的职责包括分析、数据包深层检测、逆向工程、为各种协议（DNS、DHCP、SMTP、POP、HTTP 和 VOIP）编写签名、零日攻击、Microsoft Tuesday 评论和漏洞发现。

在信息安全领域，Abhishek 喜欢研究入侵检测/防护系统、防火墙、两因素认证、无线安全、密码学和虚拟专用网。他拥有防火墙领域的发明创造并拥有一项两因素认证专利。该专利包含用户向系统的安全认证及后续的安全操作。在密码学领域，他提出了学习理论领域的一个算法，该算法使用上下文无关语法来生成一次性认证标识。一次性认证标识生

成一次性密码、可任意使用的 SSN 和可任意使用的信用卡号。为了防止高带宽和恶意转换通道，他建议在未用的 TCP/IP、UDP 和 ICMP 数据包的首部加强语义一致性。Abhishek 在编译器、计算机网络、移动代理和人工神经网络等领域的研究发现曾发表在重要会议和杂志上。

他拥有 IIT-BHU 的电子工程学士学位、乔治亚州理工大学计算学院的计算机科学和信息安全硕士学位。在求学的同时，他受雇于 Symantec 公司担任高级工程师并参与了 Cypress 通信公司的咨询项目，该项目在 2004 年 Turn Around Management 竞赛中获得第三名。他还曾在 VPN Dynamics 和 Infovation 公司工作过。

目前他和他可爱的妻子 Swati 一起住在 Banglore。

James McLoughlin（CISSP、CCSP、CCSE）是 Lan Communications 的安全工程师，这是一家爱尔兰集成商/代理商。最近，他正在为获得安全领域的 CCIE 证书而努力，他拥有 10 年安全领域的经验。

James 住在爱尔兰的都柏林。

Susan Snedaker（MBA、BA、MCSE、MCT、CPM）是 VirtualTeam Consulting, LLC（www.virtualteam.com）的首席顾问和创始人，这是一家专注于业务和技术咨询的顾问公司。该公司与各种规模的公司合作开发和实现可增加利润并促进成长的战略计划、可运作的改进和技术平台。在 2000 年创建 VirtualTeam 之前，Susan 在包括 Microsoft、Honeywell、Keane 和 Apta Software 等在内的多家公司担任过管理和技术职位。在担任 Keane 的服务交付部门经理期间，她曾管理过一支拥有超过 1200 名技术支持人员的团队，该团队通过电话和电子邮件支持不同的 Microsoft 产品，包括 Windows Server 操作系统。她是 *How to Cheat at IT Project Management*（Syngress Publishing，ISBN：1-597490-37-7）、*The Best Damn Windows Server 2003 Book Period*（Syngress Publishing，ISBN：1-931836-12-4）以及 *How to Cheat at Managing Windows Small Business Server 2003*（Syngress，ISBN：1-932266-80-1）等书的作者。她还曾为 Syngress 出版社的图书撰写过很多关于 Microsoft Windows 和安全技术方面的章节，为各种出版物撰写和编辑过技术方面的内容。Susan 曾开发和交付的技术内容包括从安全到电话、从 TCP/IP 到 WiFi、从 CIW 到 IT 项目管理以及与之相关的所有内容（她承认自己对与 TCP/IP 相关的内容有着特殊的爱好）。

Susan 拥有菲尼克斯大学的商业管理硕士学位和管理学士学位。她还拥有斯坦福大学颁发的高级项目管理证书。此外，她还拥有 MSCE（Microsoft Certified Systems Engineer）和 MCT（Microsoft Certified Trainer）证书。Susan 是南亚利桑那州信息技术协会（Information Technology Association of Southern Arizona，ITASA）和项目管理协会（Project Management Institute，PMI）的成员。

Jennifer Davis 是 Decru 公司的高级系统管理员。Decru 公司是一家网络设备公司，开发可帮助系统管理员保护数据的存储安全解决方案。Jennifer 专攻脚本开发、系统自动控制、集成、故障排除和安全管理。

目　录

第二部分 防火墙概述

第三部分 VPN 概述

第四部分 实现防火墙和 VPN（案例分析）

第1部分

安全策略

第 1 章　网络安全策略

本章内容包括：

- 定义组织
- 可信网络
- 不可信网络
- ☑ 小结
- ☑ 解决方案速查
- ☑ FAQ

1.1 引言

部署网络安全策略是一项有意义且严肃的任务。对此做出好的决定将会为网络节省大量的金钱并避免未来的许多安全问题，然而，一旦作了不正确的或是犹豫的决定，就会为不安全的网络基础架构留下隐患。创建网络安全策略将会在不同的方面影响组织，包括（但不限于）：

- **财政**　新的网络安全策略可能需要购买新设备和软件，比如防火墙、IPS（Intrusion Protection/Prevention System，入侵检测/防护系统）、防病毒软件、新路由器，以及其他等等。可能还需要为了那些受过培训后掌握了新硬件和软件的安全人员支付更多薪水。
- **网络有效性**　可能需要在网络中安装新的硬件和软件以符合新的网络安全策略，在安装和配置这些基础架构时可能会影响整个网络的有效性。因此，需要仔细计划这个过程以降低风险、开销以及客户和内部用户的宕机时间。
- **可用性**　在几乎大多数情况下，计算机系统的安全与其可用性成反比。作为网络安全策略的结果，可能会遭遇网络可用性显著下降的情况。网络安全策略需要在安全和可用性之间找到平衡，这样安全策略不会太严格以至于用户不能执行他们的日常工作。
- **法律**　根据所在国家和业务活动的不同，可能需要遵守相关的法律制度，如 HIPPA 或 Graham-Leach-Bliley。在设计网络安全策略时需要考虑这些规定。

可以开始实现新的网络安全策略之前，需要进行充分的计划和准备，然后再编写文档和配置新硬件和软件。了解网络，了解每个网络设备的原理，了解每项在用技术的弱点，了解每个设备的实力以及设备互相连接的方法，这些都很重要。

理解网络将如何使用，了解业务的需求，有多少以及什么类型的用户将访问也很关键。还需要了解为什么安装了（或要安装）网络以及是否有足够多的受过训练的员工和预算来管理网络。在任何情况下，每个网络都有其自己的需求和目标。每个网络都是不同的，在一个网络中用来降低风险的对策不会有多少可直接应用到另一个网络中。

我们很容易发现大型大学的校园网和小办公室的网络、大企业的网络和小家庭的网络之间的不同。它们都是网络，而且都会执行相同的基本操作；但是它们的安全需求却大相径庭。

正如与IT相关的大多数事情一样，在设计和实现策略和程序时，可用于加强网络安全的预算真的成问题。你的要求需要足以提供给公司和客户。有时候，生成一个每个用户都需要知道和遵循的过程，比试图实现复杂和昂贵的技术控制要更好。

许多公司现在已经意识到了需要关联的信息安全技术，以在预防、检测和响应安全措施时更加有效。而且，因为政府的规定，也要求在某些垂直行业的公司有正式成文的信息安全策略。

此外，信息安全策略对安全管理员也相当有益，因为它为确保公司信息资产的保密性、完整性和可用性提供了一个可执行级别的、经授权的框架。这意味着当安全管理员有了一纸经核准的信息安全策略后，在预算需求时就有了一定的发言权。

最后，对于安全管理员，有书面和经核准的策略可确保能够以最少中断业务的方式部署不同的技术。把书面策略视为确保正确配置一切的尚方宝剑。此外，策略是确保在有事情发生时保持工作持续的最好方法。

不管部署的是什么类型的网络，都需要脚踏实地；公司的网络需要让公司的收入比支出多。换句话说，不应在保护资产时花的钱比该资产的实际价值还要多。

在解决这个问题时，有一点也很关键：记住安全策略和安全程序的不同。网络安全策略应是高级别和相当稳定的文档，可经受住客户和服务器上所运行操作系统的相当多的变化，这样就不必在Microsoft每发布一个新服务补丁时都去发布变更。可实现网络安全过程以支持安全策略；这些过程将讨论特定操作和程序上的细节，这些细节可保证与高级别的安全策略相符。“所有接入因特网的计算机必须加以保护以免恶意入侵”是可以在安全策略中找到的指令，而“所有Windows XP计算机都必须安装SP2并启用Windows防火墙”则会是放入特定过程中的条款。

1.2 定义组织

你刚获得一份定义所在网络的网络安全策略的任务。正如在本章引言中所提到的，在定义新的网络安全策略之前需要考虑几个主题。

一个好的开始方法是好好思考一下组织。对于组织业务过程的了解有多少？既要从单个公司的角度来考虑，也要从整个行业的需要和需求来考虑。有时候，当要求信息安全工程师或顾问设计网络安全策略时，他就会意识到在开始之前必须先了解公司。

为了能够设计有用的网络安全策略，需要了解网络是为何而设计的。需要设计和部署保护公司资源安全的网络安全策略。因此，要考虑部门、业务以及公司生产和销售什么，业务是季节性的、循环的，还是说其行为在一年里都差不多。公司和国外客户、零售商或业务伙伴有业务往来吗？有任何政府部门与其业务运作有关吗？业务是否需要任何政府安全授权或许可？

比如，想象一个使用基于密码远程访问服务器的公司。网络安全策略中提到适当的过程以防忘记密码吗？或者用户知道是否要打电话给老板、IT 部门或者甚至是信息安全办公室来获得新密码吗？

在有良好定义的网络安全策略的公司里，用户将有可循的过程来获得新密码。这个过程需要足够安全以保证密码给到正确的人而不是入侵者。

密码恢复过程需要保护，但是也要足够灵活以使得即使不在办公室或远程办公时，用户也可恢复密码并继续工作。可以考虑使用电话安全检查或其他离线方法来重设密码。

要定义“典型”的组织几乎是不可能的，因为所有公司都各不相同。因此，需要开发一种方法来定义自己的组织。可选择几个原则，比如公司的规模、地理位置和执行的不同活动等等。不管使得公司与其他公司不同的特质如何，都应发展自己的网络安全策略，以作为保护公司资产并同时使得它可完成所需任务的方法，而不仅仅是关注于关闭端口和定义因特网访问等等。在可以建立网络安全策略之前，应先执行公司及其资产的安全评估。这个过程有两个不同的部分：审计和评估。评估试图发现在安全破坏之前可减轻、修补或消除的问题和脆弱性。审计通常在评估之后进行，其目的是测量与策略和过程相符的程度。典型地，有人对审计结果负责。有些人不喜欢审计这个词，可能这太容易让人想起山姆大叔的所作所为，他还在追查你三年前的税单，当时你声称某次度假是出差，因为你在等待去海滨酒店的巴士时给老板打了个电话。

虽然术语评估和审计通常可交替使用，本章我们更为关注的是评估。

在整个评估和审计阶段，记住 IT 安全主要有三个组成部分：人、过程和技术。需要解决所有这三个领域的一个平衡方法；仅关注于某个领域而不考虑其他领域会产生安全漏洞。人，包括高级管理人员，必须理解安全的重要性，而且必须理解和参与到对其维护之中。过程包括为了保持网络安全出现和重复出现的所有实践和程序。技术显然包括构成网络基础架构的硬件和软件。技术评估的某些部分要求评估和加强基础架构安全，包括部署公司的正确技术解决方案。在 IT 界，我们通常过度关注保护技术所花的时间和精力，而忽视了人和过程对整个安全环境的重要性。

为了保护基础架构的安全，需要理解其建筑分区。这包括：

- 网络边界保护
- 内部网络保护
- 入侵监视和防护
- 主机和服务器配置
- 防范恶意代码
- 事故响应能力
- 安全策略和过程
- 雇员的意识和培训
- 物理安全和监视

安全评估应从检查要在其中实现安全的整个环境开始。因为需要在安全和信息危险程度之间寻求平衡，所以检查公司信息的重要程度是个很好的起点。作为这个分析的一部分，还需要检查网络基础架构入侵的影响，以及防范和修复该类事件的代价。需要定义所拥有的不同的适当的系统，并查看信息在公司中是如何流动的，以理解试图要保护的基础架构。最后，还需要创建初始评估范围已定义什么包含及什么不包含在项目中。

1.2.1　信息危险程度

从查看信息危险程度开始很重要。你会发现在大多数安全文献中，这是一个共同的主题，因为保护没有人需要的信息是毫无意义的。信息危险程度是对网络拥有什么以及在整个计划中它们有多重要的评估。所有数据创建时不是都相等的，如果公司生产喂马的铁槽，那么很有可能，这个网络中的数据不会和在线股票经纪公司或银行或信用卡处理机构网络中的数据那样吸引潜在的攻击者。因此，需要检查信息的危险程度以决定要花费多少来保护这些信息。没有人希望破坏安全，但是花 1500 万美元来保