Cisco职业认证培训系列
CISCO TRAINING SOLUTION

著:
〔美〕Michael Wenstrom

译:
李逢天　李原慧
张　帆　刘兴初

管理CISCO网络安全

MANAGING CISCO NETWORK SECURITY

Learn how to secure your network
with the official MCNS Coursebook

CISCO SYSTEMS
CISCO PRESS
www.ciscopress.com

人民邮电出版社
www.pptph.com.cn

Cisco 职业认证培训系列

管理 Cisco 网络安全

[美] Michael Wenstrom 著

李逢天 李原慧 张 帆 刘兴初 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

管理 Cisco 网络安全 / （美）温斯特姆（Wenstorm, M.）著；李逢天等译.
—北京：人民邮电出版社，2001.11
（Cisco 职业认证培训系列）
ISBN 7-115-09718-6

I. 管… II. ①温… ②李… 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（2001）第 069368 号

Cisco 职业认证培训系列
管理 Cisco 网络安全

◆ 著　[美] Michael Wenstrom
译　李逢天　李原慧　张　帆　刘兴初
责任编辑　刘　涛

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ pptph.com.cn
网址　http://www.pptph.com.cn
读者热线　010-67129212　010-67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787 × 1092　1/16
印张：39.5
字数：948 千字　2001 年 11 月第 1 版
印数：1 - 4 000 册　2001 年 11 月北京第 1 次印刷

著作权合同登记　图字：01 - 2001 - 0776 号
ISBN 7-115-09718-6/TP·2514

定价：75.00 元

内容提要

基于同名的培训课程，《管理 Cisco 网络安全》一书集中介绍了如何实施 IP 网络的安全。

本书分为六个部分。第一部分教给读者如何建立网络安全策略和保护网络基础设施方面的信息。第二部分描述用 CiscoSecure ACS 和 Cisco IOS 软件 AAA 安全特性来保护远程拨号访问安全的方法。第三部分集中讲述通过识别边界安全系统的基本组件和配置边界路由器及 Cisco 防火墙特性集来保护 Internet 访问安全。第四部分向读者介绍 PIX 防火墙的特性和组件，提供了有关如何配置基本 PIX 防火墙特性的详细信息。第五部分剖析 Cisco 加密技术（CET），并教给读者如何配置 CET 来确保数据私密性。在第六部分中，读者将学习如何用 IP 安全（IPSec）特性来实施一个安全的虚拟专用网络（VPN）解决方案，以及如何使用入侵检测和网络统计工具。

本书是 MCNS 培训课程的正式教材，同时也适合作为广大网络管理人员的参考书，用以设置、维护网络安全。

版权声明

关于作者

Mike Wenstrom 是 Cisco Systems 公司的培训专员，他设计、开发和交付关于 Cisco 虚拟专用网络（VPN）和网络安全产品方面的培训。

他选择了在通信技术领域为提高人们的知识和技能提供培训和指导，作为他的职业。他尤其喜欢将复杂的技术题目转换成人们容易理解的形式。Mike 在技术培训方面有 18 年以上的经验，他做过指导设计人、课程开发人、技术指导人和项目经理。

在硅谷的 21 年生涯中，Mike 工作过的公司有：Cisco Systems、Aspect Communications、Siemens、IBM、ROLM、Tymnet、NCR 和美国海军。他现在与妻子和女儿住在德克萨斯州的奥斯汀，为 Cisco 的 VPN 和网络安全产品开发培训并教学。他毕业于 Western Illinois 大学，获得文学学士学位。他在电子技术方面有 AS 学位，并是一位 CCNA（Cisco 认证的网络助理）。

J.T. Agnello，在过去的 15 年里，他一直在德克萨斯州的奥斯汀作为一名系统管理员，曾为很多中小型、直到大型企业，如 Sematech、Schlumberger、IBM 等等，执行系统及网络运维和管理。在过去 3 年中，他一直在撰写技术培训课程，为例如 Tivoli Systems（IBM 所收购的一家公司）、Pervasive Software 等公司提供了覆盖例如系统、网络、安全和数据库管理等题目的培训课程。

Scott Morris 是 Mentor Technologies 公司（原 Chesapeake Computer Consultants 公司）的一位指导/顾问。他在涉及计算机和网络的很多不同领域工作过。通过获得 Novell 认证证书、Microsoft 认证证书和 Cisco 认证证书。

其他为本书编写做出贡献的作者

在 Cisco 技术方面，Scott 是一名 Cisco 认证的系统指导教师（Cisco Certified System Instructor ，CCSI），是路由和交换方面的 CCIE（CCIE 证号为 4713），是路由和交换方面的 CCDP，并是广域网交换方面的 CCNA。Scott 原来教授“Cisco 互联网络故障排除”（CIT）课程，但他喜欢尝试教授新课程，为了从中找到乐趣。

Cary A. Riddock，在过去一年里为佛罗里达州中部的一家大型健康管理公司做网络工程师。他的职责包括监视公司的局域网/广域网，并解决与连通性有关的故障。现在，他正忙于一种使用 PKI 和基于令牌卡（token card）的认证技术、允许公司管理人员通过公共 Internet 访问私有内部网络（intranet）应用的系统。Cary 拥有下列证书：MCSE、CCNA、CCDA、CCDP 和 CCA。

关于技术审稿人

本书的审稿人为《管理 Cisco 网络安全》一书的整个开发过程贡献了他们自己相当多的实际经验。

Richard Benoit 为一家总部位于佛罗里达州的奥兰多的国际娱乐集团公司任网络和技术项目经理。现在，他的工作重点是在企业网络设计、管理和安全方面。从前，作为顾问，他为顾客提供大型网络设计、实施和支持方面的服务。他所获得的网络证书包括 CCNP（加上安全）、CCDA 和 Microsoft 的 MCSE。

Doug MacBeth 是 Cisco Systems 公司的一位 IOS 文档管理经理。他在技术文档管理方面有 15 年以上的工作经验，从 1993 开始就在 Cisco Systems 公司工作。在 Cisco 公司的工作经历中，他曾为 Cisco IOS 文档集做过编辑和项目领导人。

Doug McKillip，P.E.，CCIE＃1851，是 Global Knowledge 公司在 Cisco 认证培训方面的一位独立顾问。他在计算机网络领域有 12 年以上的工作经验，在过去 8 年中，他积极参与研究安全和防火墙技术。在 MCNS 版本 1.0 培训课程的最初部署过程中，Doug 提供了指导性的和技术性的帮助。他是 Global Knowledge 公司（Cisco Systems 公司的一家培训合作伙伴）的主要指导教师和课程总监。

Hank Mauldin 是 Cisco Systems 公司的顾问工程师，工作在 CTO 办公室。他已经在 Cisco 工作了好几年，从事评估和设计数据网络方面的工作。他的专业领域包括 IP 路由协议、服务质量（QOS）和网络安全。Hank 现在是 Cisco Network Designer（一种网络设计工具）的程序经理。在加入 Cisco 之前，他曾为几家不同的系统集成商工作过。他有 15 年以上的数据网络工作经验。

致　　谢

MCNS 课程是一个团体项目，在 Cisco 公司内、外有很多贡献者，包括 Cisco 课程开发人员、课程编辑和指导教师。虽然我是 MCNS 课程的主要课程开发者，但我要感谢使这门课程成功的其他人员的重要努力，包括作为 Cisco 课程指导教师的 Tom O'Hara、Sean Coville 和 Kevin Calkins，作为课程顾问和设计师的 Hank Mauldin 和 Chris Lonvick，作为重要的 Cisco 培训合作伙伴培训教师的 Doug Mckillip，作为课程编辑的 Brian Adams 和 Deborah Lewis，以及作为最初的 MCNS 项目经理的 Chris Berriman。

开发 MCNS 这本书是一个困难但很有益的项目。我想要感谢我的经理，Rick Stiffler，和安全培训组中我的同事们，他们容忍了我多次前一天晚上为本书忙碌到凌晨 2 点之后再来上班。我还想要感谢 Cisco Press 的工作人员，他们努力帮助我按计划完成本书。特别表扬 Kitty Jarett 和 Brett Bartow，他们在整个项目过程中耐心地和我及其他作者一起工作。我感谢技术审稿人所做的重要贡献，并感谢使本书成功的其他作者。

序　言

《管理 Cisco 网络安全》以书的形式讲解了同名的认证准备课程里所包括的全部主题，这门由讲师指导的课程是很有挑战性的。MCNS 将传授给读者所需的知识和技能，以便能在 IP 网络中安装、配置、操作、管理和验证 Cisco 网络安全产品及 Cisco IOS 软件安全特性。读者将学习如何识别网络安全威胁，如何用 CiscoSecure ACS 和 Cisco IOS AAA 特性保护远程拨号接入访问的安全，如何用 Cisco 边界路由器和 PIX 防火墙保护 Internet 访问的安全，以及如何用 IPSec 实施安全的 VPN。无论是为了准备 Cisco 在安全方面的专业认证，还是想实际了解一下 Cisco 网络安全解决方案，这本书所提供的信息都将使读者获益匪浅。

为了给我们的客户和更广泛的用户群体提供另一个学习工具，Cisco 和 Cisco Press 将这些内容以课本的形式介绍给大家。尽管一本书不能复现由讲师指导的环境，但是我们相信不同的人对于同一种教授方式的反应是不同的。我们通过 Cisco Press 出版物提供这些内容的目的是希望将这些知识传授给更广泛的网络互联专业人员。

Cisco 将通过这些教科书讲授现有的和未来的课程，以帮助实现 Cisco “Internet 学习解决方案组”的主要目标：培训 Cisco 网络互联专业技术人员群体，使该群体能够组建和维护可靠的、可扩展的网络。Cisco 职业认证以及支持这些认证的课程就是要通过有计划的循序渐进的学习来实现这些目标。Cisco Press 与 Cisco Systems 合作出版的这些书在内容和质量方面都达到了我们课程和认证所要求的标准。我们的目的是使读者在构筑其网络互联知识库的过程中发现本书及随后的 Cisco Press 认证和培训出版物都是极有价值的。

Cisco Systems 公司
Internet Learning Solutions Group 副总裁
Thomas M. Kelly
2000 年 7 月

作者序

因为网络攻击事件的不断出现，且人们已意识到 Internet 革命会继续存在并将是国家和个人繁荣发展的关键，所以计算机和网络安全已经成为了重要的新闻。全世界范围内的国家和公司领导人已经开始重视对网络安全的急迫需求。很多人已经意识到，他们的网络甚至缺乏最基本的安全措施，而且也缺少训练有素的网络专业人员来实施网络安全。

致力于提高网络专业人员的知识和能力水平的培训教师当中的很多人都看到了这个需求：为了帮助人们开始更好地保护他们的网络安全，应该创建一套完整的方法以教授网络安全知识。我们看到了推动人们进入网络安全领域、让更多的人能发展他们的安全专业水平的需求，这样才能从整体上提高网络安全水平。所以我们决定创建一门新的网络安全课程以解决我们所预见到的需求问题。

早在 1997 年，作为 Cisco 全球培训部门的一名课程开发人员，我被我当时的经理 Chris Berriman，指派来开发“管理 Cisco 网络安全（MCNS）”课程。尽管那时还没有人提出要学这门课程，但我们的小组已经预见到将来对网络安全培训的需求肯定会有爆炸性的增长。那时我还做了一个非正式的竞争课程调研，发现没有一家公司提供这样的课程。

本课程是为了帮助大家纵览 Cisco 网络安全技术，在所提供的知识面广度和每个题目的覆盖深度上做了一个平衡。课程中要求动手的实验练习将有助于读者巩固概念和事实。MCNS 项目已经启动了，是团队集体的努力导致了 MCNS 第 1 版和后续版本的产生。

本书与 MCNS 培训课程在内容上是平行的，但它已根据所做的广泛研究被完全重写。今天，对一本全面的网络安全书籍的需求是非常强烈的。本书的目的是为了培训更多的网络安全专业人员和助理以满足对至关重要的网络安全的需求，并使网络安全对更多的人变得可用和可以理解。

Cisco Systems 公司
Mike Wenstrom
2000 年 8 月

前　言

本书的目标是为了帮助读者实现 Cisco 所支持网络安全技术、设计和实现更安全的网络。本书被设计作为 MCNS 培训课程的补充教材，也可以作为一本独立的参考书。

本书的读者对象

本书是为那些想要了解 Cisco 网络安全特性和技术的读者所写的。主要面向那些需要扩展其路由和交换技术以外领域的知识和在安装、配置、监测及核验 Cisco 网络安全产品和特性方面提高能力的网络专业人员。本书假定读者已具有通过 CCNA 认证考试所需要的 Cisco 网络知识水平。

本书的第二类目标读者是那些需要了解网络安全威胁以及如何减少这些威胁的一般用户。本书用一种对用户友好的方式解释了很多网络安全概念和技术，这种方式对那些喜欢非纯技术性手册的读者应该比较有吸引力。

本书的特性

本书有一些能帮助读者学习和将本书中所介绍的网络安全题目用于实际工作的独特之处：

- **包括的概念**——在每一章的开头有本章所涵盖主题列表；
- **图、例和表格**——本书有一些图、例子和表格，它们用一种易于使用的形式展示了每一章中的内容。图能够帮助解释概念和软件运行过程，例子为命令和输出结果提供了样例，表格提供了对诸如命令句法之类事实的描述；

- **案例学习**——XYZ 公司，一个假设的企业，被用在每一章中，以使各配置示例形成一个统一的整体，并让这些示例看起来更真实。基于 XYZ 公司的网络安全策略样例被贯穿于整本书中，作为如何实施网络安全策略指示的一个模型。基于 XYZ 客户环境，很多章中的案例学习中的网络样例总结了该章所讲授的配置信息。
- **命令汇总**——本书将命令汇总放在了每个专题中，而没有单独作为一个章节，是为了便于读者学习和应用所提供的任务；
- **各章小结**——在每一章末尾都有一个该章所讨论概念的汇总。它提供了每一章的大纲，可作为学习帮助；
- **复习题**——每章的小结之后都有 10 道复习题，用于巩固各章所介绍的概念，它们可帮助读者测试学习效果。各章的复习题答案在附录 D 中提供；
- **参考文献**——复习题之后是与本章所介绍主题相关的参考文献列表。它们可帮助读者对本章所讲授内容之外的知识进行扩展。

本书所用的表示习惯

本书使用下列表示习惯。

- 重要的术语或新术语用斜体字表示；
- 所有代码示例以类似于屏幕字体的等宽字体显示，代码的各个部分用下列表示习惯：

——命令和关键字用加粗体表示；
——斜体字表示用户应输入具体值的参数；
——方括号[ ]表示任选关键字或参数；
——大括号{ }表示必选项；
——竖线(|)用于分开待选项；

本书的组织

本书分为七个部分，包括 18 章和 4 个附录。

第一部分：建立网络安全策略

第 1 章，“评估网络安全威胁”，通过检查一个企业网络的潜在威胁，回答了“我们为什么需要网络安全”这个根本问题。它详述了网络安全的挑战和网络安全脆弱性的 3 个主要原因。它还描绘了网络入侵者的嘴脸，并讨论了网络安全威胁的 4 个主要种类和相应的防御工具。

第 2 章，“评估网络安全策略”，讨论了保护网络安全的经济因素，勾画出了网络安全策略的主要组成部分。它还总结了 Cisco 所做的一个网络安全调研，并包括一个读者可以评估安全策略样例的练习。

第 3 章，“保护网络基础设施的安全”，讲授了如何配置 Cisco 路由器以保护园区网络环境安全。它包括：保护管理接口的安全、控制对网络设备的 SNMP 访问、防止来自闯入者的路由更新的方法、控制网络数据流量的简单方法，以及控制以太网交换机端口和访问安全。

第二部分：拨号（dialup）安全

第 4 章，“分析 Cisco AAA 安全技术”，讨论了 AAA 的架构和与其相关的技术。它介绍了有助于实施 Cisco 产品中可获得的 AAA 安全解决方案的概念。

第 5 章，“配置网络接入服务器使用 AAA 安全特性”，讨论了如何配置一台 Cisco 网络接入服务器以允许 AAA 进程使用一个本地或远程的安全认证数据库。此外，还介绍了如何排除与 AAA 进程相关的故障。

第 6 章，“配置 CiscoSecure ACS 和 TACACS+/RADIUS”，讨论了用于 Microsoft Windows NT 和 UNIX 平台的 CiscoSecure ACS 的特性和架构。此外，它还描述了如何在 NT 上配置 CiscoSecure ACS 为 Cisco 网络接入服务器执行 AAA 功能，重点是 TACACS+协议的使用。

第三部分：保护 Internet 连接安全

第 7 章，“配置 Cisco 边界路由器”，介绍了如何利用 Cisco 路由器的安全特性创建网络边界安全系统。它包括对网络边界安全组件和对边界安全有用的 Cisco IOS 软件特性的概述；本章还教给读者如何使用每一种特性来保护网络边界安全。

第 8 章，“配置 Cisco IOS 防火墙”，讨论如何利用 Cisco 路由器上的 Cisco IOS 防火墙特性集来增强网络边界安全。它包括对基于上下文的访问控制概述，并教给读者如何在一个网络边界安全系统中配置 IOS 防火墙。

第四部分：配置 CiscoSecure PIX 防火墙

第 9 章，“PIX 防火墙基础”，讨论了 Cisco PIX 防火墙系列的能力、特性及配置选项。它向读者展示了：即使仅用一个基本的配置命令集，PIX 防火墙也能提供强大的安全功能。

第 10 章，“配置通过 PIX 防火墙访问”，在第 9 章的基础之上，讨论了如何用具体的配置命令控制通过 PIX 防火墙的进入访问和外出访问。它包括如何配置网络地址翻译、静态翻译，以及其他访问控制方法。

第 11 章，“在 PIX 防火墙上配置多个接口和 AAA”，讨论了如何灵活地在 PIX 防火墙上配置多个接口以创建一个更安全的停火区（DMZ）。它还介绍了如何配置 PIX 防火墙的 AAA 特性以便与 CiscoSecure ACS 协同工作、启用用户级的访问控制。

第 12 章，“配置 PIX 防火墙高级特性”，讨论了 PIX 防火墙的一些更特别的特性，这些特性使 PIX 防火墙在控制 Internet 访问和特性方面不仅功能强大而且非常灵活。本章还介绍了 PIX 防火墙对 PPTP 的支持、对 Java applet 的阻挡、URL 和 FTP 过滤、对 SNMP 和 syslog 的支持、PIX 防火墙的冗余性和维护特性。

第五部分：配置 Cisco 加密技术

第 13 章，“Cisco 加密技术概览”，讨论了在 Cisco 路由器上配置 Cisco 加密技术所需的概念。它介绍了加密算法、散列（hashing）技术、数字签名，以及与 Cisco 加密技术一起使用的密钥交换方法。

第 14 章，“配置 Cisco 加密技术”，介绍了在 Cisco 路由器上配置 Cisco 加密技术必须完成的任务和步骤。它介绍了用于配置和测试 Cisco 加密技术的 Cisco IOS 命令，这些命令是按进入它们启用该特性的次序组织的。

第六部分：配置 IPSec VPN

第 15 章，“理解 Cisco 对 IPSec 的支持”，给出了 IPSec 及在 Cisco 产品中可用于创建 VPN 的 IPSec 协议的概述。本章介绍了 IPSec 中的每一种协议。后续各章提供了在 Cisco 产品中如何配置 IPSec 支持的细节。

第 16 章，“配置 Cisco IOS IPSec”，讨论了在一个站点到站点型的拓扑结构中，如何为预共享密钥和 RSA 加密认证在 Cisco 路由器中配置 IPSec。通过分解成独立的任务和步骤，本章简化了我们配置 IPSec 所必须遵守的复杂过程。

第 17 章，“配置 PIX 防火墙对 IPSec 的支持”，讨论了在一个站点到站点型的拓扑结构中，如何为预共享密钥认证在 PIX 防火墙中配置 IPSec。它介绍了配置 IPSec 的任务和步骤，示出了启用该特性需要的所有命令。

第 18 章，“扩展 Cisco IPSec 网络”，描述了如何配置 Cisco 路由器和使用 IPSec 的 PIX 防火墙组成的 Cisco IPSec 网络，让它们在保持安全性的同时能扩展支持多个 IPSec 对等体。它包括如何配置证书授权支持和 Cisco VPN 客户端远程访问。

第七部分：附录

附录 A，“XYZ 公司案例学习背景介绍”，描写了 XYZ 公司的案例学习，以帮助将贯穿本书所讨论的安全概念和实施流程联系起来。它提供了各章样例配置中所用的 IP 地址和网络设备。

附录 B，“XYZ 公司网络安全策略的一个例子”，包含贯穿本书所用的 XYZ 公司网络的网络安全策略一个示例。它包括为 XYZ 公司解决企业网络安全主要问题的策略声明。

附录 C，“配置标准和扩展访问控制列表”，总结了 Cisco IOS 访问控制列表，它们对 Cisco 路由器中的很多安全特性是非常重要的基础。它包括标准和扩展 IP 访问控制列表中所用的命令。

附录 D，“复习题答案”，给出了各章末尾复习题的答案。

目　录

第一部分　建立网络安全策略

第二部分　拨号(Dialup)安全