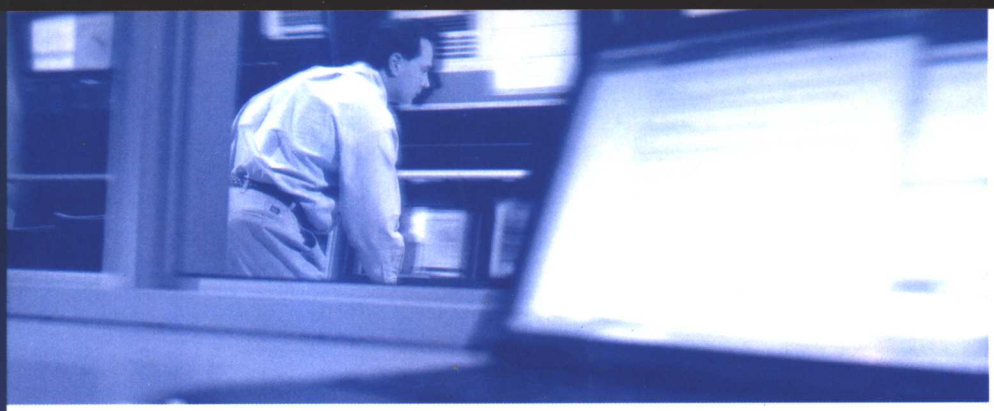
Cisco Systems

Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com



# CCSP 自学指南：安全 Cisco IOS 网络 (SECUR)

# CCSP Self-Study:

## Securing Cisco IOS Networks (SECUR)

Cisco authorized self-study book for
CCSP® 642-501 foundation learning

[美] John F. Roland 著
张耀疆 陈克忠 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

# CCSP 自学指南：安全 Cisco IOS 网络（SECUR）

[美] John F. Roland 著

张耀疆 陈克忠 译

人 民 邮 电 出 版 社

**图书在版编目（CIP）数据**

CCSP 自学指南：安全 Cisco IOS 网络（SECUR）/（美）罗兰（Roland, J.F.）著；张耀疆，陈克忠译. —北京：人民邮电出版社，2005.2
（Cisco 职业认证培训系列）

ISBN 7-115-12985-1

Ⅰ. C… Ⅱ. ①罗… ②张… ③陈… Ⅲ. 计算机网络－安全技术－工程技术人员－资格考核—自学参考资料 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 140866 号

**版 权 声 明**



Cisco 职业认证培训系列

**CCSP 自学指南：**

**安全 Cisco IOS 网络（SECUR）**

◆ 著 [美] John F.Roland
译 张耀疆 陈克忠
责任编辑 李 际

◆ 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 ciscobooks@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
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：36. 5
字数：1 053 千字 2005 年 2 月第 1 版
印数：1-3 500 册 2005 年 2 月北京第 1 次印刷

著作权合同登记 图字：01 - 2004 - 0565 号

ISBN 7-115-12985-1/TP • 4385

定价：75.00 元

**本书如有印装质量问题，请与本社联系 电话：（010）67129223**

# 内容提要

本书全面系统地介绍了在基于 Cisco 路由器的网络环境中，如何实施和管理网络安全。全书共 13 章，从内容上可以分成 5 个部分。第一部分包括第 1 章到第 4 章，详尽地介绍了网络安全的基本概念和相关 Cisco 路由器的基本的安全配置；第二部分包括第 5 章到第 7 章，介绍了 3 种 Cisco IOS 的增强功能——防火墙特征集；第三部分包括第 8 章到第 10 章，介绍了怎样利用 Cisco 路由器建立和管理 VPN；第四部分包括第 11 章到 13 章，介绍了两种 Cisco 网络安全的管理工具——安全设备管理器（SDM）和路由器管理中心（MC），以及一个全面地配置 Cisco 路由器的综合案例；附录部分给出了章节复习题答案、网络安全策略样例和访问控制列表参考。

本书是 Cisco Press 出版的关于 CCSP 的官方教材，是 CCSP 应试者的必备书籍。同时本书内容翔实，涉及知识面广，也适合广大网络管理人员和网络爱好者阅读与参考，更全面、更有效地保护自己的网络安全。

# 关于作者

**John F. Roland**，CCNA，CCDA，CCNP，CCDP，CSS-1，MCSE，是 WesTek 顾问公司的一名安全专家。从 IBM 大型机上的 COBOL 编程到局域网/广域网设计和实施（美国军方网络），一直到最近开发 Cisco 及微软认证培训材料，John 已经在 IT 领域从业 22 年了。目前，John 受托为一家大型的电缆通信公司设计技术培训材料。

John 拥有 Tiffin 大学会计学士学位，在 General Motors 研究所辅修数学和电子工程。

## 关于技术编辑

**Leon Katcharian** 是 Cisco Systems 公司的一名教育专家，负责设计开发 Cisco 网络安全培训产品。Leon 在数据安全领域具有 19 年的工作经验，是一名技术支持工程师、一名技术讲师、一名技术作家以及课程开发者。

**Jay Swan** 负责讲授 Cisco Global Knowledge 课程，是一名认证的 Cisco Systems 讲师，拥有 Stanford 大学的学士和硕士学位。在加入 Global Knowledge 之前，Jay 工作于 ISP 和更高的教育领域。Jay 持有 CCNP 和 CCSP 证书。

**Dale Tesch Jr.** 是 Cisco Systems 东北渠道小组的一名高级技术工程师，拥有计算机信息系统（CIS）学士学位，持有 CCNP 和 CISSP 证书。

## 关于译者

**张耀疆**，CISSP，CISA，BS7799LA，ITILFoundation，MCSE+Internet，MCSD，CCNA，信息安全专业硕士，资深信息安全咨询顾问和培训讲师，著有《聚焦黑客——攻击手段与防护策略》，

另有译著《CISSP 认证考试指南》，目前担任上海安言信息技术有限公司（www.aryasec.com）CTO。负责本书前 4 章的翻译。电子邮件：colababy@263.net.cn。

**陈克忠**，CCNP，从事 Cisco 网络的设计、部署、维护和安全优化工作，具有多年电信级网络的实践经验，长期担任 Cisco 网络安全课程讲师。翻译本书第 5 章到第 13 章、附录 A、B、C 和术语表。

# 献　词

本书献给我的妻子 Mariko、我的儿子 Michael，是他们长期的支持、持久的爱和鼓励才促使我能够完成此书。我爱你们！

——John F.Roland

# 致　谢

我特别要感谢 Cisco Press 的 Michelle Grandin，他在本书问世过程中给予我极大的信任和帮助。Michelle 以多种方式帮助我，总是不吝鼓励之言，与她工作的这几个月真的非常愉快。

Dan Young 在此书出版过程中提供了不倦的编辑反馈、指导、支持和鼓励，他对此书所做的贡献真的难以计数，跟他共事真的非常高兴。感谢你。

此外，我也想对此书的技术审稿人 Leon Katcharian、Jay Swan 和 Dale Tesch Jr.表示感谢，要不是他们的评价、建议和严谨的态度，此书很难成为有价值的资源。感谢你们所有的人！

# 序

本书是一部 Cisco 权威认可的自学工具，可以帮助读者理解 SECUR 考试所覆盖的基本概念。本书由 Cisco Internet 学习方案组（Cisco Internet Learning Solutions Group）以及 Cisco 负责开发 SECUR 考试的小组协作完成。作为考试初期准备的材料，本书介绍了识别安全威胁的必要知识以及使用 Cisco IOS 安全特性的必要技能。无论是想通过学习而取得 CCSP 认证资格，还是只想寻求对加强 Cisco IOS 路由器网络安全有用的产品、服务及策略的更好的理解，读者都会从本书提供的信息中获益。

Cisco 公司和 Cisco Press 期望通过这种文字格式的出版物向客户以及广大的用户群体提供一种卓有成效的学习工具。尽管简单的一部出版物还不足以取代讲师授课或者电子学习的方式，但必须承认，并非每个人都对单一的授业机制表现出相同的反映。我们的意图是，通过 Cisco Press 来交付这些材料，将极大地增强知识在更广泛受众中传播的力度。

Cisco Press 还将提供其他与现有和未来考试相关的认证自学系列书籍，以便实现 Cisco Internet 学习方案组的原则目标：教育网络专家的 Cisco 群体，促使该群体建立并维护可靠的、规模化的网络。Cisco 职业认证和支持这些认证的课程所秉持的方向，正是通过严格的积极学习的途径来满足这些目标的。

为了在 Cisco 职业认证方面取得成功，也为了按照 Cisco 认证专家的标准来履行自己的日常职责，我们建议大家采用混合式的学习方法，将讲师授课培训、实际操作经验、电子学习以及自学紧密结合起来。Cisco 公司授权给遍布全球的 Cisco 学习伙伴，他们可以提供最具资格的授课以及最大价值的动手经验（实验室和仿真环境）。为了了解更多有关 Cisco 学习伙伴程序的情况，特别是与读者所在区域相关的情况，请参阅下列站点 http://www.cisco.com/go/authorizedtraining。

本书是 Cisco Press 协同 Cisco 公司创建的，满足课程和认证的内容标准要求，我们期望，读者在搭建自己的网络知识基石的时候，能够真正领略到本书以及后续 Cisco Press 认证自学书籍的价值。

Thomas M. Kelly
Cisco Systems 公司 Internet 学习方案组
2004 年 3 月

# 作者序

网络安全是许多年来大多数组织都非常关注的问题，从最初的“管理 Cisco 网络安全”（Managing Cisco Network Security，MCNS）课程，到现在这门课程，都因为安全这个热点问题而被广泛接受。这些精心设计的课程为网络工作者提供了最关键的信息，使其能够从容应对日益增多的网络威胁。MCNS 课程是以前的 Cisco 安全专家（CSS-1）课程表中的一个组成部分。

因为客户要求有一个专家级的安全课程，Cisco 对最初的 CSS-1 课程进行了重新设计，建立了新的 Cisco 认证安全专家（Cisco Certified Security Professional，CCSP）课程体系。重新设计后的 MCNS 课程就成为了 Cisco IOS 网络安全（Securing Cisco IOS Network，SECUR）课程，这正是本书的基础。

John F. Roland
WesTek 顾问公司
2004 年 3 月

# 前　言

本书的目标是帮助读者实施 Cisco IOS 网络安全技术，创建高度可管理且安全的网络。本书专为 Cisco SECUR 课程而设计，也可以作为独立参考材料。

## 期望读者群

本书适合于任何想要了解 Cisco 网络安全特性和技术的人员。主要的目标受众是需要扩展路由选择及交换技术知识，并且需要用 Cisco IOS 软件及 Cisco IOS 防火墙的强大特性来提升安装、配置、监视和校验 Cisco 网络安全技能的网络专家。本书假定读者已经具备与通过 CCNA 认证考试同等的 Cisco 网络知识。

第二个目标受众是需要理解网络安全威胁及其对策的一般用户。本书介绍了许多网络安全的概念和技术，讲述方式非常友好，不会让读者有参考技术手册那样的晦涩感。

## Cisco 认证安全专家

如果读者有意获取专业证书，可以通过 Cisco 所要求的系列认证考试来向当前或者预期的雇主或伙伴证明自己的能力。许多网络专家都追崇 CCSP 证书，因为网络安全已经日益成为 21 世纪商业活动全面安全计划中非常关键的一个要素。本书就是设计用来帮助读者取得这一享有极高声望的证书的，如果它就是你的目标的话。

CCSP 认证是一个主流的思科认证方向，始于 CCNA，终止于 CCIE，就像 CCNP、CCDP 和 CCIP 认证那样。CCSP 认证需要你通过 5 门考试。完成这些考试并获取 CCSP 证书的前提条件是你必须持有一张 CCNA 证书。表 I-1 包含了一列 CCSP 认证系列的考试科目。

CCSP 证书有效期是 3 年，之后必须履行再认证的要求。目前，再认证的要求是重新参加最新版本的适当的考试。在 Cisco.com 上可以看到很多关于 CCSP 的信息。

表 I-1 CCSP 认证考试

| 考试号 | 建议参加的培训 |
| --- | --- |
| 642-501 SECUR | **Securing Cisco IOS Networks（SECUR）（前身是 MCNS）v1.0**<br>5 天课程，讲授用于加强 Cisco IOS 路由器网络安全的知识和技能 |
| 642-511 CSVPN | **Cisco Secure Virtual Private Networks（CSVPN）v3.1**<br>4 天课程，讲授用于描述、配置、校验和管理 Cisco VPN 3000 集线器、Cisco VPN 软件客户端、Cisco VPN 3002 硬件客户端特性集的知识和技能 |
| 642-521 CSPFA | **Cisco Secure PIX Firewall Advanced（CSPFA）v3.1**<br>4 天课程，讲授用于描述、配置、校验和管理 PIX 防火墙产品系列的知识和技能 |
| 642-531 CSIDS | **Cisco Secure Intrusion Detection Systems（CSIDS）v3.0**<br>3 天课程，讲授用于设计、安装和配置为小型、中型及企业网络提供的 Cisco 入侵保护方案的知识和技能，此外，也学习管理和监视 IDS 的方法 |
| 642-541 CSI | **Cisco SAFE Implementation（CSI）v1.1**<br>4 天课程，讲授用于在特定设备上实施和使用“SAFE: Extending the Security Blueprint to Small, Midsize and Remote-User Networks”白皮书的知识和技能 |

Cisco 建议取得 CCSP 证书最好是参加由 Cisco 培训伙伴提供的培训课程。表 I-1 描述了所推荐的课程，这些课程都是围绕数小时的实验操作而设计的，可以让学员体会到实际配置或管理所学设备的经验。

# 本书特点

本书具有诸多特色，有助于读者掌握本书覆盖的网络安全内容：

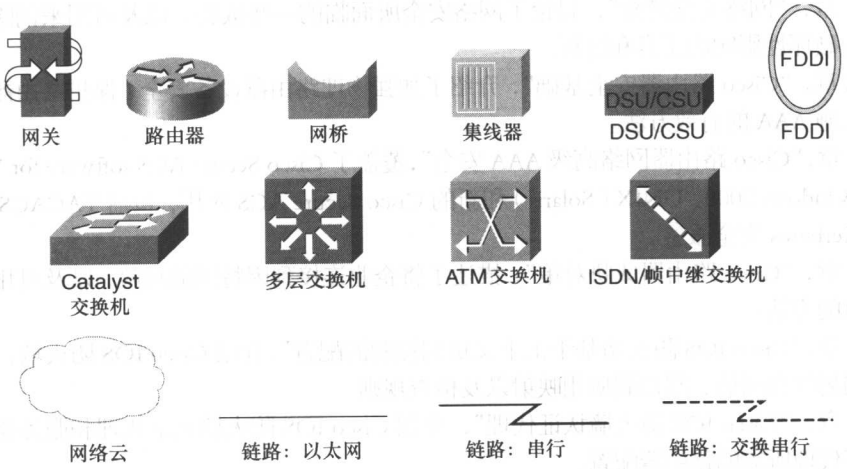
- **概念**——在每一章的开始处都会列出本章覆盖的话题，这提供了对相关概念的参考，可用作高效的组织。
- **图、例子和表格**——本书每个章节都包含图片、例子和表格，这使得章节内容易读易懂。图片用来解释概念和软件过程，例子提供了命令和输出的示例，表格提供了诸如命令语法和描述的知识。
- **案例研究**——未来公司，一家假设的企业，在本书每个章节都会提及，它是配置示例的落脚点，这使得全书例子的组织浑然一体并且更近现实。一个基于未来公司的例子网络安全策略贯穿全书，成为实施安全策略指导的一个模型。许多章节中的案例研究网络示例都是对本章讲述的配置信息的归纳总结，当然，其基础也是未来公司的客户环境。
- **命令概要**——每小节都包含命令概要，易于学习和任务实践。
- **章节小结**——在每一章的最后都有一个对本章讲述概念的总结，可以作为章节大纲，有助于学习。
- **复习题**——在每一章的小结后面，都会有 10 个或者更多的问题，这些问题可以促进对本章讲述概念的记忆，有助于在知新之前先行温故。问题答案都在附录 A 中。
- **术语表**——术语表提供了对本书用到的关键术语的简洁解释。

# 本书组织

本书一共包括 13 章、3 个附录和一个术语表。

- 第 1 章，“网络安全简介”，讨论了网络安全所面临的一些威胁，以及可用来消除这些威胁和潜在破坏性影响的工具和过程。
- 第 2 章，“Cisco 路由器安全基础”，介绍了加强物理路由器设备安全、保护路由器管理接口以及实施 AAA 的有效方法。
- 第 3 章，“Cisco 路由器网络高级 AAA 安全”，覆盖了 Cisco Secure ACS software for Windows NT 或 Windows 2000、UNIX（Solaris）和新的 Cisco Secure ACS 应用，包括 TACACS+、RADIUS 和 Kerberos 安全服务。
- 第 4 章，“Cisco 路由器威胁对策”，描述了将企业连接到因特网的风险，以及可用来消减这些风险的方法。
- 第 5 章，“Cisco IOS 防火墙基于上下文访问控制的配置”，介绍 Cisco IOS 防火墙，讨论 CBAC、全局超时和阈值、端口到应用映射以及检查规则。
- 第 6 章，“Cisco IOS 防火墙认证代理”，介绍 Cisco IOS 防火墙认证代理和服务器，以及支持认证代理所需的路由器配置。
- 第 7 章，“Cisco IOS 防火墙入侵检测系统”，介绍针对 Cisco 路由器的 Cisco IOS 防火墙入侵检测系统包，及其配置方法。
- 第 8 章，“用 Cisco 路由器和预共享密钥建立 IPSec VPN”，介绍用预先共享密钥认证来配置 Cisco IOS IPSec 的方法。
- 第 9 章，“用 Cisco 路由器和 CA 建立高级 IPSec VPN”，介绍用 CA 对 Cisco IOS IPSec 的配置。
- 第 10 章，“用 Cisco Easy VPN 配置 IOS 远程接入”，介绍使用 Cisco Easy VPN 和 Cisco VPN 客户端来配置 Cisco IOS 远程接入。
- 第 11 章，“使用安全设备管理器保护 Cisco 路由器”，介绍和说明 Cisco 安全设备管理器。
- 第 12 章，“管理企业 VPN 路由器”，介绍和说明 Management Center for VPN Routers（Router MC）。
- 第 13 章，“案例研究”，最大程度上利用本书讨论过的大多数安全要素。
- 附录 A，“各章复习题答案”，提供了每章最后复习题的答案。
- 附录 B，“网络安全策略实例”，包含针对未来公司网络的网络安全策略的例子。
- 附录 C，“配置标准和扩展访问列表”，概览在 Cisco IOS 软件中配置标准和扩展 IP 访问列表。
- 术语表提供了对本书涉及的术语的简洁解释。

## 本书用到的图标




## 命令语法约定

本书在命令语法的表示上与 Cisco IOS 命令参考的约定相同：

- **黑体字** 指出字面显示的命令和关键字。在实际的配置例子和输出（并非一般的命令语法）中，黑体字指出用户手工输入的命令（例如 **show** 命令）；
- *斜体字* 指出需要提供实际值的参数；
- 竖线（|） 分隔替换项，相互排斥的元素；
- 方括弧（[ ]） 指出可选元素；
- 大括弧（{ }） 指出必须的选择；
- 带方括弧的大括弧（[{ }]） 指出在一个可选元素中的必须的选择。

# 目　录