



Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com



CCSP Cisco 安全 VPN 认证考试指南

CCSP™ Self-Study

CCSP Cisco Secure VPN Exam Certification Guide

Official self-study test preparation guide for the
Cisco 9E0-121 and 642-511 CSVN exams

内附光盘



[美] John F. Roland 著
Mark J. Newcomb
白建军 王宝生 译

 人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

CCSP Cisco 安全 VPN 认证考试指南

John F. Roland

[美]

著

Mark J. Newcomb

白建军 王宝生 译

人民邮电出版社

图书在版编目 (CIP) 数据

CCSP Cisco 安全 VPN 认证考试指南 / (美) 罗兰 (Roland, J. F.), (美) 纽坎博 (Newcomb, M. J.) 著; 白建军, 王宝生译. —北京: 人民邮电出版社, 2003.12

ISBN 7-115-11225-8

I. C... II. ①罗... ②纽... ③白... ④王... III. 计算机网络—完全技术—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 (2003) 第 090446 号

版 权 声 明

John F.Roland Mark J.Newcomb: CCSP Self-Study CCSP Cisco Secure VPN Exam Certification Guide

Copyright © 2003 by Cisco Systems, Inc.

All rights reserved.

本书中文简体字版由美国 Cisco Press 出版公司授权人民邮电出版社出版。未经出版者书面许可, 对本书的任何部分不得以任何方式复制或抄袭。

版权所有, 侵权必究。

Cisco 职业认证培训系列

CCSP Cisco 安全 VPN 认证考试指南

- ◆ 著 [美] John F.Roland Mark J.Newcomb
译 白建军 王宝生
责任编辑 陈 昇
- ◆ 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: 26
字数: 622 千字 2003 年 12 月第 1 版
印数: 1-4 000 册 2003 年 12 月北京第 1 次印刷

著作权合同登记 图字: 01-2003-1078 号

ISBN 7-115-11225-8/TP · 3421

定价: 58.00 元 (附光盘)

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

关于作者

John F.Roland, CCNA、CCDA、CCNP、CCDP、CSS-1、MCSE, 是一位为 Ajilon 咨询公司工作的安全专家。John 在 IT 业中工作了 22 年, 从事过 IBM 大型机上 COBOL 程序的开发和美国军方网络的 LAN/WAN 的设计与实现, 最近从事 Cisco 开发和 Microsoft 认证培训教材的编写。John 当前的职位是在美国一家大银行中负责设计和实现企业级网络认证测试。

John 在俄亥俄州的 Tiffin 大学获得了会计学学士学位, 并在歇根州 Flint 的通用汽车研究所辅修了数学和电子工程专业。

Mark J.Newcomb 是华盛顿 Spokane 安全网络公司的拥有者, 也是首席安全工程师。Mark 具有 20 年以上的网络行业工作经验, 他一直关注金融和医疗行业。最近 6 年开始为太平洋西北岸的广大客户设计安全解决方案。Mark 是第一批从 Cisco 获得 CCNA 证书的人, 还获得了 CCDA、CCNP 和 CCDP 证书。他是 *Cisco Internet Security Solutions* (Cisco Press 出版) 一书的合著者, 他还有两本其他的网络著作。他曾经作为技术审稿人, 为很多出版社审核了 20 多本网络方面的图书。

关于技术审稿人

Scott Chen 已经在 IT 界工作了 7 年，并担任过不同的职位，包括资深 NT 工程师、资深网络工程师和首席网络工程师/网络经理。Scott 目前是 Triad 金融公司的首席网络工程师/网络经理，该公司隶属于 Ford 汽车公司。他曾经为多家企业实现了远程访问和 LAN-to-LAN 的 VPN 解决方案。Scott 有丰富的企业网络设计、实现和支持经验，熟练掌握 Cisco 公司提供的各种技术，包括路由、交换、安全、内容交换、无线、BGP、EIGRP 和 NAT。Scott 毕业于加利福尼亚大学 Irvine 分校，获得学士学位。他拥有很多资格认证，如 MCSE、CCNA、CCNP 和 CCIE 笔试。

Gert Schauwers 是一位拥有 3 个 CCIE 证书（CCIE No.6942）——路由与交换、安全及通信与服务。他有 4 年以上的互联网工作经验，获得电子/通信工程师资格。Gert 目前在 Brussels CCIE 实验室工作，他是路由与交换、安全及通信与服务考试的学监及内容工程师。

Thomas Scire 从 1996 年开始为网络基础设施行业工作。Thomas 专长于 LAN、WAN、安全，以及 Cisco Systems、Checkpoint 和诺基亚的多业务基础架构。Thomas 为 Accudata 系统公司工作，该公司是一家独立的 IT 专业服务公司，主要是企业网络和安全基础设施。他所从事过的著名项目包括企业 VPN、IP 电话配置和帧中继网络上的国际语音配置。Thomas 从 Polytechnic 大学获得计算机工程学士学位，还获得了许多职业认证证书，如 Cisco CCNA/CCDA、Cisco IP 电话设计专家、Checkpoint 认证安全工程师、Checkpoint 认证安全教师和 Nokia 安全管理员。

献 辞

John Roland:

谨以此书献给我结婚 28 年的妻子 Mariko 和我的儿子 Michael, 感谢他们的理解和支持。他们永恒的爱和鼓励使我在本书的写作中能够集中精力。你们太伟大了! 我还要把此书献给我已过世的双亲, Hazel 和 Forrest Roland, 感谢他们抚养了我, 教育了我, 为我树立了无私的爱榜样, 指导我取得今天的成绩。我相信他们会永远被人们所怀念。

Mark Newcomb:

谨以此书献给我的妻子 Jacqueline 和我的女儿 Isabella Rumiana。当我写作时 Jacqueline 的耐心和理解令我佩服。

致 谢

John Roland:

写作本书使我有机会与一些非常优秀的人一起工作。我要感谢 Cisco Press 的 Brett Bartow, 感谢他对本项目的信念和努力。我还要感谢 Cisco Press 的 Michelle Grandin 编辑的支持。Michelle 在该项目中从许多方面帮助我, 一直对我进行鼓励。Cisco Press 的 Dayna Isley 提供了开发手册和回复, 使我工作没有太多的障碍, 感谢她将工作转为专业的文档。在这几个月里与你们 3 位一起工作是非常愉快的。

其次, 我要感谢我的合著者 Mark Newcomb。感谢他在我因个人问题不能工作时完成本书另一半的工作。谢谢你, Mark。你的专业水准和专家意见使本项目终于开花结果。

我还要感谢技术审稿人 Gert Schauwers、Scott Chen 和 Thomas Scire。感谢他们的意见、建议和对细节的关心。没有他们的帮助, 本书不可能像今天这样有价值。谢谢你们大家。

Mark Newcomb:

我衷心感谢 John Roland 对本书的贡献, 感谢他邀请我参加本书的编写。没有任何文字能够表达我的心情。有过将近 5 年的写作、技术审校以及与不同出版社打交道的经历, 我要赞扬 Cisco Press 的每一位员工。我在 Cisco Press 认识了 Michelle Grandin、Dayna Isley、John Kane 和 Brett Bartow, 他们的专业精神值得我们尊重。我特别要感谢 Tammi Ross。在任何组织中, 总有一个人能够解决任何不能解决的问题。Tammi 证明了她就是 Cisco Press 中的那个人。

Cisco Press 的技术审稿人都是世界级的。技术审稿人是一个优秀出版社最有价值的资产。他们得不到他们应得的赞誉和酬谢。感谢 Gert Schauwers、Scott Chen 和 Thomas Scire。他们的努力使本书能够具有今天的成绩。

前言

Cisco Systems 的系列认证为读者提供了评价读者在某个核心学习领域专业技术的有效方法。许多网络专家正在努力获得 Cisco 认证安全专业人员 (CCSP) 认证, 因为网络安全已经成为 21 世纪企业中总体安全计划中极其重要的部分。本书就是为了帮助读者获得这个在业界享有盛誉的认证。

目标和方法

本书的主要目标是帮助那些要获得 CCSP 认证或 VPN 认证的读者通过 9E0-121 或 642-511 Cisco 安全 VPN (CSVPN) 考试。作为个人, 我们会通过不同媒介保留信息, 基于上述前提, 本书提供了许多方式帮助读者通过考试。问题构成了本书的重要部分, 因为它们是读者在考试中要面对的, 而且它们也是衡量读者理解材料的有效手段。附带的光盘提供了附加的问题帮助读者准备考试。

除了书和光盘中广泛、全面的问题之外, 本书还详细地覆盖了所有公布的考点, 并使用了图、表和截屏图来帮助读者理解概念。本书假定读者已经具备了一定的网络知识 (Cisco 要求参加 CCSP 认证的首要条件就是拥有 CCNA 证书, 然后再通过 5 门考试), 不会用读者应该掌握的材料来烦扰读者。某些知识点强调读者必须具备一些 CCNA 认证没有提供的知识时, 本书会补充这些知识使读者掌握这部分知识点。由于这是认证考试指南, 因此目标是给读者足够的信息理解公布的主题并通过考试, 考试中的主题相关的材料是有效的和精简的。

本书能够帮助读者使用如下方法通过 Cisco Secure VPN 考试:

- 每章开始有自我评估问题帮助读者发现需要学习的地方。
- 提供了详细的主题材料向读者澄清没有理解的地方。

- 每章末尾的练习和场景研究（scenario）帮助读者确定从本章中学到了什么。
- 光盘中附加的问题向读者提供了从不同角度对待材料的机会。

谁需要阅读本书

本书旨在帮助读者通过 CCSP Cisco 安全 VPN 考试。因为这是本书的主要目标，显然 CCSP 的应试者将会从本书中受益。每个要获得 CCSP 认证的人都必须参加 Cisco 安全 VPN 考试，本书将使您受益匪浅。

这并不意味着这又是一本考试辅导资料，通过考试后就可以丢入垃圾箱。本书中的材料提供的 VPN 配置挑战的实际解决方案有 80%~90% 你会在日常网络工作中遇到。本书对于安全网络经理是非常有价值的参考工具。设计者也可以从中找到有价值的材料和结论用于网络设计项目。

本书的内容组织

尽管可以一页一页地阅读本书，但是本书的结构非常灵活。您可以在章节之间任意移动，选择自己需要用到的材料。第 1 章提供了 CCSP 证书的概述，给出了准备考试的策略。第 2 章到第 11 章是核心章节，可以以任意顺序阅读。如果您打算阅读所有的章节，书中的顺序是一个可以使用的很好的顺序。

核心章节——第 2 章到第 11 章——覆盖了以下考点：

- **第 2 章，“VPN 及 IPSec 技术概述”**——这一章讨论了 VPN 协议和概念，重点在 VPN 协议上。本章覆盖的考试内容如下：
 - 1 Cisco 产品实现安全 VPN；
 - 2 IPSec 概述；
 - 3 IPSec 协议框架；
 - 4 IPSec 如何工作。
- **第 3 章，“Cisco VPN 3000 系列集中器硬件概述”**——本章着眼于 Cisco VPN 3000 系列集中器，并描述了每个 VPN 集中器型号的性能。本章覆盖的考试内容如下：
 - 5 Cisco VPN 3000 系列集中器概述；
 - 6 Cisco VPN 3000 系列集中器模型；
 - 7 Cisco VPN 3000 系列集中器的优点以及特性；
 - 8 Cisco VPN 3000 系列集中器客户端支持。
- **第 4 章，“为使用预共享密钥的远程访问配置 Cisco VPN 3000”**——本章描述了为使用预共享密钥的远程访问配置 VPN 集中器的过程。集中器的最初的 CLI 和浏览器配置也包含在内。同时讨论了高级配置问题。为 Windows 安装和配置 Cisco VPN 客户端也在本章中进行了讨论。本章覆盖的考试内容如下：
 - 9 使用预共享密钥的远程访问概述；
 - 10 用于远程访问的 Cisco VPN 3000 系列集中器的初始化配置；
 - 11 Cisco VPN 3000 系列集中器的浏览器配置；
 - 12 配置用户和组；

- 13 Cisco VPN 3000 系列集中器的高级配置;
- 14 配置 IPSec 的 Windows 客户。
- **第 5 章, “为使用数字证书的远程访问配置 Cisco VPN 3000”**——本章讨论了数字证书和证书授权委员会 (CA) 支持。注册和安装证书, 生成公共/私有密钥对, 确认证书也被讨论。本章中, VPN 集中器和 VPN 客户端被配置使用数字证书。本章覆盖的考试内容如下:
 - 15 CA 支持概述;
 - 16 证书生成;
 - 17 证书确认;
 - 18 为 CA 支持配置 Cisco VPN 3000 集中器系列。
- **第 6 章, “配置 Cisco VPN 防火墙功能”**——本章讨论了 VPN 客户端的防火墙特性设置, 包括 Are You There 特性、中心策略保护和监控防火墙统计。本章覆盖的考试内容如下:
 - 19 软件客户端的防火墙功能概述;
 - 20 软件客户端的 Are You There 功能;
 - 21 软件客户端的有状态防火墙功能;
 - 22 软件客户端的中心策略保护功能;
 - 23 客户端的防火墙统计;
 - 24 自定义防火墙策略。
- **第 7 章, “监控和管理 VPN 3000 系列集中器”**——本书中的前面章节讨论的都是 VPN 管理器的配置菜单。本章将继续 VPN 管理器的剩余部分, 监控和管理员部分。本章覆盖的考试内容如下:
 - 25 监控 Cisco VPN 3000 系列集中器;
 - 26 管理 Cisco VPN 3000 系列集中器。
- **第 8 章, “配置 Cisco 3002 硬件客户端进行远程访问”**——本章全面讨论 Cisco VPN 3002 硬件客户端。交互和集成的硬件和客户端认证将会被讨论。客户端统计监视也将在本章中涉及到。本章覆盖的考试内容如下:
 - 27 Cisco VPN 3002 硬件客户使用预共享密钥进行远程访问;
 - 28 VPN 3002 交互单元身份认证和用户身份认证功能概述;
 - 29 配置 VPN 3002 集成单元身份认证功能;
 - 30 配置 VPN 3002 用户身份认证;
 - 31 监控 VPN 3002 用户统计。
- **第 9 章, “配置 VPN 3002 硬件客户的可扩展功能”**——Cisco VPN 3002 硬件客户端也很好地区适用于大型组织。本章讨论了负载均衡的可扩展性、PAT、自动升级和备份服务器。本章覆盖的考试内容如下:
 - 32 VPN 3002 硬件客户反向路由注入 (Reverse Route Injection) 概述;
 - 33 配置 VPN 3002 备份服务器功能;

——34 配置 VPN 3002 负载平衡功能;

——35 VPN 3002 自动升级功能概述;

——36 配置 VPN 3002 自动升级功能;

——37 监控 VPN 3002 自动升级事件;

——38 端口地址转换概述;

——39 配置基于 UDP 的 IPSec;

——40 配置基于 TCP 的 IPSec。

- 第 10 章,“具有预共享密钥的 Cisco VPN 3000 局域网对局域网”——作为远程访问的理想实现, Cisco VPN 3000 系列集中器对于 LAN-to-LAN VPN 连接也是一个优秀的平台。本章将讨论 LAN-to-LAN 的概念, 并且向您演示如何配置 VPN 集中器来实现这个功能。本章覆盖的考试内容如下:

——41 Cisco VPN 3000 IPSec 局域网对局域网;

——42 局域网对局域网配置;

——43 SCEP 支持概述;

——44 根证书安装;

——45 身份证书安装。

- 第 11 章,“场景研究”——本章给出了测试你分析各种 VPN 环境并且应用你的知识来解决问题实现方案的能力。

书中所用图标



路由器



多层交换



交换机



PIX 防火墙



ATM 交换机



内容交换机



路由器/交换机
处理器



Cisco 7500
系列交换机



ISDN 帧中继
交换机



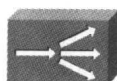
Hub



网桥



NetRanger
入侵检测系统



本地控制器



访问
服务器



Cisco 安全
扫描器



IP/TV
广播
服务器



Cisco
呼叫管理器



Cisco
目录服务器



PC



膝上型电脑



Cisco Works
工作站



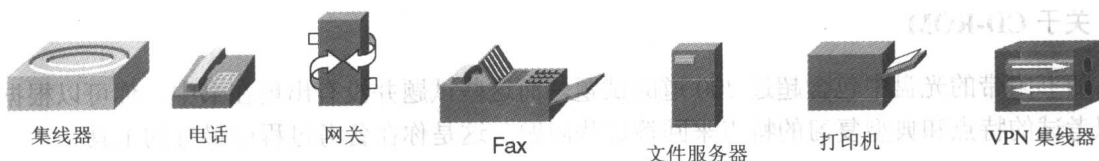
Web
浏览器



Web
服务器



网云



命令语法惯例

本书中所用的命令语法惯例同 IOS 命令参考中所使用的约定相同。下面给出命令参考给出的惯例描述：

竖线 (|) 隔开多个相互独立的可选参数。

方括号 [] 表示可选参数。

大括号 {} 表示一个必需的选择项。

方括号内的大括号 [[]] 表示在一个可选参数内的必须选择项。

黑体表示按所显示的逐字输入的命令和关键字。在实际的配置实例和输出（不是一般的命令语法）中，**黑体**表示用户手工输入的命令（例如一个 **show** 命令）。

*斜体*表示你所提供的实际值的论据。

各章的特点

例示的测试问题允许进行最终考试的模拟。后续的每一章都有一些共同的特点来帮助你该章最有效地利用你的时间。主要有以下特点：

- **“我已经知道这些了吗？”测验和分类测试**——每一章都以一个测验开始，它将有助于你决定你在本章将花费多少时间。测验又被分为小节，称为“分类测试”，与该章的一部分对应。在每一章的开始部分后面紧跟着的是“我已经知道这些了吗？”以引导你是学习本章的全部内容还是部分内容。
- **基础知识点**——这是各章的核心，主要解释协议、概念和本章话题的配置。
- **基础知识小结**——接近本章的最后，总结了本章最重要的图表。这部分主要是帮助你复习本章的关键概念，如果你在“我已经知道这些了吗？”测验小节得的分数较好的话，而且那些概念是最后复习时最值得看的内容。
- **Q&A**——这些在各章最后的问题主要集中于通过几种类型的问题来复习在“基础知识点”一节介绍的内容。因为“我已经知道这些了吗？”测验中的问题同样能够有助于你的复习，这些问题又在 Q&A 部分稍微重复一点。重新回顾这些问题，并考虑一些新的问题，将为你提供很多实际的问题以测试你在阅读完本章后所掌握的知识，也非常有助于在最终考试到来前进行最后的复习。
- **场景研究**——在大多数章节的最后。场景能够给你一个对真实网络实施的深入介绍。而不是仅问一些简单的问题以获取一些事实。场景使你能够不用根据多选测验的形式来设计和构建自己的网络（至少是在纸上）。

关于 CD-ROM

随书附带的光盘中包含超过 200 道的试题，而这些试题并没有出现在书中。你可以根据模拟考试的特点和典型复习的特点来回答这些问题。这是你在备考过程中最好的工具。

目 录

第 1 章 关于 Cisco 认证安全专业人员	3
1.1 这本书如何帮助你通过 CCSP Cisco 安全 VPN 考试	5
1.2 CCSP 认证概述及需要的考试	5
1.3 Cisco 安全 VPN 考试	6
1.4 关于 Cisco 安全 VPN 考试的主题	7
1.5 推荐的适合于 CCSP 认证的培训途径	8
1.6 使用本书来通过考试	9
1.7 最后的考试准备技巧	9
第 2 章 VPN 及 IPSec 技术概述	13
2.1 如何最好地使用本章	14
2.2 “我已经知道这些了吗？”测验	14
2.3 Cisco VPN 产品线	17
2.4 通过 Cisco 产品实现 VPN 应用程序	17
2.4.1 典型的 VPN 应用	17
2.4.2 使用 Cisco 的 VPN 产品	21
2.5 IPSec 协议概述	28
2.5.1 IPSec 协议	30
2.5.2 安全关联	35
2.5.3 在 IPSec 过程中使用的已有协议	36
2.5.4 认证 IPSec 对等实体并形成安全关联	41
2.5.5 协议与转换集结合	41
2.6 使用 IPSec 建立 VPN	43
2.6.1 Step 1: 感兴趣的流量触发 IPSec 处理过程	45
2.6.2 Step 2: 认证对等实体并建立 IKE SA	46
2.6.3 Step 3: 建立 IPSec SA	46
2.6.4 Step 4: 允许安全通信	47
2.6.5 Step 5: 终止 VPN	47

2.7 与 IPSec 一同使用的协议表格	47
2.8 IPSec 预配置过程	48
2.9 使用 IPSec 创建 VPN	49
第 3 章 Cisco VPN 3000 系列集中器硬件概述	57
3.1 如何最好地利用本章	58
3.2 “我已经知道这些了吗？”测验	58
3.3 Cisco VPN 3000 系列集中器的主要优点	61
3.3.1 配置及使用的简易性	62
3.3.2 性能及可扩展性	63
3.3.3 安全性	65
3.3.4 容错	67
3.3.5 管理接口	68
3.3.6 升级简单	72
3.4 Cisco 安全 VPN 集中器：比较以及特性	72
3.4.1 Cisco VPN 3005 集中器	73
3.4.2 Cisco VPN 3015 集中器	74
3.4.3 Cisco VPN 3030 集中器	75
3.4.4 Cisco VPN 3060 集中器	75
3.4.5 Cisco VPN 3080 集中器	76
3.4.6 Cisco VPN 3000 系列集中器 LED 指示器	76
3.5 Cisco 安全 VPN 客户端特性	78
3.5.1 Cisco VPN 3002 硬件客户端	79
3.5.2 Cisco VPN 客户端	79
3.6 Cisco VPN 3000 集中器表	80
3.7 Cisco VPN 3000 集中器能力表	81
第 4 章 为使用预共享密钥的远程访问配置 Cisco VPN 3000	91
4.1 如何最好地使用本章	92
4.2 “我已经知道这些了吗？”测验	93
4.3 使用 VPN 进行带有预共享密钥的远程访问	96
4.3.1 惟一预共享密钥	96
4.3.2 组预共享密钥	97
4.3.3 通配符预共享密钥	97
4.4 VPN 集中器配置	97
4.4.1 Cisco VPN 3000 集中器配置需求说明	98
4.4.2 Cisco VPN 3000 集中器初始化配置	99
4.4.3 通过 VPN 3000 集中器系列管理器配置带有预共享密钥的 IPSec	111
4.4.4 VPN 集中器的高级配置	123
4.5 安装和配置 VPN 客户端	127

4.5.1 VPN 客户端概述	127
4.5.2 VPN 客户端特性	127
4.5.3 VPN 客户端安装	129
4.5.4 VPN 客户端配置	132
4.6 预共享密钥的类型	135
4.7 VPN 3000 集中器的 CLI 快速配置步骤	136
4.8 VPN 3000 集中器基于浏览器的管理器快速配置步骤	136
4.9 VPN 客户端安装步骤	137
4.10 VPN 客户端配置步骤	137
4.11 VPN 客户端程序选项	137
4.12 组和用户数目的限制	138
4.13 全部的配置目录	138
4.14 全部的管理目录	140
4.15 全部的监督目录	140
4.16 场景研究 4-1	150
4.17 场景研究 4-2	150
4.18 场景研究 4-1 答案	151
4.19 场景研究 4-2 答案	152
第 5 章 为使用数字证书的远程访问配置 Cisco VPN 3000	155
5.1 如何最好地使用本章	156
5.2 “我已经知道这些了吗？”测验	157
5.3 数字证书和证书授权委员会	159
5.3.1 CA 的体系结构	159
5.3.2 简单证书注册过程的身份认证方法	164
5.3.3 支持 Cisco VPN 产品的 CA 供应商和产品	166
5.4 通过 VPN 3000 系列集中器管理器提供数字证书支持	167
5.4.1 证书生成和注册	167
5.4.2 证书确认	170
5.4.3 废弃证书 (revocation) 列表	171
5.4.4 IKE 配置	172
5.5 为 CA 支持配置 VPN 客户端程序	174
5.6 PKCS # 10 证书请求字段	176
5.7 X.509 身份证书字段	176
5.8 数字证书类型	176
5.9 CA 组织类型	177
5.10 证书确认和身份认证过程	177
5.11 基于 Internet 的证书颁发机构	177
5.12 证书管理应用程序	177
5.13 场景研究 5-1	182

5.14 场景研究 5-2.....	182
5.15 场景研究 5-1 答案	182
5.16 场景研究 5-2 答案	183
第 6 章 配置 Cisco VPN 客户端的防火墙功能.....	185
6.1 如何最好地使用本章	186
6.2 “我已经知道这些了吗？”测验	186
6.3 Cisco VPN 客户端防火墙功能概述	189
6.4 防火墙配置概述	191
6.4.1 有状态防火墙（总是开启）功能	191
6.4.2 Are You There 功能	192
6.5 配置防火墙过滤器规则	192
6.5.1 名字、说明和操作	195
6.5.2 协议和 TCP 连接	195
6.5.3 源地址和目的地址	196
6.5.4 TCP/UDP 源端口和目的端口	196
6.5.5 ICMP 分组类型	197
6.6 配置有状态防火墙	197
6.7 为使用防火墙配置 VPN 集中器	198
6.7.1 防火墙设置	199
6.7.2 防火墙	199
6.7.3 自定义防火墙	199
6.7.4 防火墙策略	200
6.8 监视 VPN 客户端防火墙统计	200
6.9 启用通过 Cisco VPN 3000 系列集中器管理器自动升级客户端	202
6.10 Cisco VPN 客户端防火墙功能概述	203
6.11 有状态防火墙（总是开启）功能	205
6.12 Cisco 集成客户端	205
6.13 中心保护策略	205
6.14 Are You There 功能	205
6.15 配置防火墙过滤器规则	206
6.16 操作（Action）	207
6.17 配置有状态防火墙	207
6.18 为使用防火墙配置 VPN 集中器	207
6.19 防火墙	208
6.20 防火墙策略	208
6.21 监视 VPN 客户端防火墙统计	208
6.22 场景研究 6-1	211
6.23 场景研究 6-1 答案	211