Cisco Systems
Cisco Press
Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS
CQS

Cisco安全虚拟专用网络

Cisco Secure Virtual Private Networks

Plan,deploy,and maintain Virtual Private Networks with the official CSVPN Coursebook

Andrew G. Mason 著
李逢天 姜莹 张伟 张帆 译

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

Cisco 职业认证培训系列

Cisco 安全虚拟专用网络

Andrew G. Mason 著

李逢天 姜莹 张伟 张帆 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

Cisco 安全虚拟专用网络/（ ）梅森（Mason, A. G.）著；李逢天等译.
—北京：人民邮电出版社，2002.8
ISBN 7-115-10365-8
Ⅰ. C... Ⅱ. ①梅...②李... Ⅲ. 虚拟网络 Ⅳ. TP393
中国版本图书馆 CIP 数据核字（2002）第 043454 号

版权声明

Cisco 职业认证培训系列

Cisco 安全虚拟专用网络

◆ 著 Andrew G. Mason
译 李逢天 姜 莹 张 伟 张 帆
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 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67180876
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：20.25
字数：485 千字 2002 年 8 月第 1 版
印数：1-4 000 册 2002 年 8 月北京第 1 次印刷

著作权合同登记 图字：01-2001-4100 号
ISBN7-115-10365-8/TP・2920
定价：42.00 元

内容提要

本书详细介绍了在实际的网络环境中规划、部署和管理VPN所需的知识。全书共分为12章，分别介绍了VPN和IPSec的基本概念；Cisco的VPN产品系列；在Cisco IOS路由器和Cisco PIX防火墙上如何应用预共享密钥和数字证书来配置IPSec的场点到场点型VPN，以及相应的故障排除技术；如何安装VPN 3000系列集中器，以及如何应用预共享密钥和数字证书来为远程接入进行配置；VPN集中器的管理和监测技术；可用于IPSec VPN的扩展性解决方案。在本书每一章的开头都给出了明确的学习目标，并在每一章的结尾提供了一组复习题，用以评估读者对本章知识的掌握情况。贯穿全书有很多例子和详细的图表，可以帮助读者更清晰地了解文中所介绍的概念。

本书是针对有一定基础的、具有系统管理实际经验的读者。对于那些了解安全VPN在其基础设施中的需要且正在进一步学习网络互联方面知识的初学者，本书也照顾到了。本书涵盖了Cisco考试9EO-570 CSVPN所要求的内容，可以帮助考生获得Cisco认证。

关于作者

Andrew G. Mason 是三家英国公司的首席执行官，三家公司分别是 Mason Technologies, CCStudy.com,和 Boxing Orange 公司，他获得的 IT 认证有 CCIE #7144、CSS-1、CCNP: Security 和 CCDP。他专长于为许多公司提供与 Cisco 公司的产品与技术有关的咨询服务。Andrew 在网络业界有 11 年的工作经验，现在在为英国最大的 ISP 提供技术咨询工作。他每日潜心于利用 Cisco Secure 产品系列来设计和实施复杂的安全解决方案。

关于技术审稿人

Kelly McGrew 是 mcgrew.net 公司的副总裁，这是一家进行网络培训和课程开发的公司。他还是一名 CCSI（Cisco Certified Systems Instructor）。他在世界范围内进行培训工作。Kelly 拥有语音接入方面的 CCNP（Voice Access Specialist）和 CCDA 认证。他在网络业界有超过 15 年的工作经验，还具有在当今以 IP 为中心的网络世界很少遇到的各种 LAN 和 WAN 协议的工作经验。Kelly 在网络业界已担任过很多职务。包括：CompuServe Network Services 和 MCI/WorldCom 公司的网络系统工程师、Chesapeake Computer Consultants 公司的指导教师/顾问、微软公司的程序经理，以及 Cisco Systems 公司的指导教师/顾问。Kelly 现在致力于基于第二层或 IP 层（第三层）的语音技术的教学和课程开发。

Mark J.Newcomb 拥有 CCNP：Security 和 CCDP 证书，是 Aurora Consulting Group 公司(www.auroracg.com)的高级网络咨询工程师，这是一家位于华盛顿州 Spokane 的公司，是 Cisco 的高级合作伙伴。Mark 为西北太平洋地区的客户提供网络设计、安全和实施服务。

Mark 在微型计算机业界有超过 20 年的工作经验。他现在的工作包括为无线装置设计安全的通信系统，以及为银行系统提供全面的安全服务。

前　言

《Cisco 安全虚拟专用网络》是一本全面的、面向结果的书，意图向读者提供关于虚拟专用网络（VPN）的规划、管理和维护方面的基本知识。通过阅读《Cisco 安全虚拟专用网络》这本书，读者将能够完成很多具体任务，包括：

- 了解 Cisco 安全 VPN 产品的特性、功能和优点。
- 了解在 Cisco 安全 VPN 产品中所实现的组件技术。
- 掌握在 Cisco IOS 软件中配置和测试 IPSec 时需要的过程、步骤及命令。
- 掌握在 Cisco 安全 PIX 防火墙中配置和测试 IPSec 时需要的过程、步骤及命令。
- 安装和配置 Cisco VPN 客户端，以创建一条通往 Cisco VPN 集中器和 PIX 防火墙的安全隧道。
- 配置和验证 Cisco VPN 集中器、Cisco 路由器和 Cisco 安全 PIX 防火墙中的 IPSec。
- 为了协同工作而配置 Cisco VPN 集中器、Cisco 路由器和 Cisco 安全 PIX 防火墙。

总之，读者将不仅仅了解到 VPN 的理论知识（和 VPN 的明显优点），也将能够通过详细的步骤学会实际的配置方法。这将让读者能立刻在他们的实际工作环境中应用 VPN 技术。

本书的每一章都有鲜明的主题。无论是理论还是实践，读者都将能以一种对成人学习非常有效的、清晰、简练的方式从每一章中获得知识。本书也提供了很多图解，为文字部分做了很好的补充。

本书面向的对象

《Cisco 安全虚拟专用网络》是针对有一定基础的、具有系统管理实际经验的读者。对于那些了解安全 VPN 在其基础设施中的需要且正在进一步学习网络互联方面知识的初学者，

本书也照顾到了。最主要的读者是打算使用已经到位或即将购买的设备来实施 VPN 解决方案的系统管理员。本书也适用于希望拓宽知识面的学生——帮助他们通过 Cisco 认证。本书涵盖了 Cisco 考试 9EO-570 CSVPN 所要求的内容。

本书的内容是假设读者非常熟悉一般的网络概念和技术。这包括对网络协议 TCP/IP 的完整理解。

本书的主要内容

本书分为 12 章：

- 第 1 章，“VPN 和 VPN 技术”——本章是对 VPN 的概述并详细地介绍了 IPSec。
- 第 2 章，“Cisco VPN 产品系列”——本章介绍了 Cisco 产品线中可用于建立虚拟专用网络的产品。
- 第 3 章，“配置 Cisco IOS 路由器应用预共享密钥（场点到场点）”——本章着重讲述了在 Cisco IOS 路由器上如何使用预共享密钥配置 IPSec 场点到场点的 VPN。
- 第 4 章，“配置 Cisco IOS 路由器应用 CA（场点到场点）”——本章着重讲述了在 Cisco IOS 路由器上如何使用数字证书配置 IPSec 场点到场点的 VPN。
- 第 5 章，“Cisco IOS VPN 的故障排除”——本章介绍了可用于 Cisco IOS VPN 故障排除的排错工具和技术。
- 第 6 章，“配置 Cisco PIX 防火墙应用预共享密钥（场点到场点）”——本章着重讲述了在 Cisco 安全 PIX 防火墙上如何使用预共享密钥配置 IPSec 场点到场点的 VPN。
- 第 7 章，“配置 Cisco PIX 防火墙应用 CA（场点到场点）”——本章着重讲述了在 Cisco PIX 防火墙上如何使用数字证书配置 IPSec 端到端的 VPN。
- 第 8 章，“Cisco PIX 防火墙 VPN 的故障排除”——本章介绍了可用于 Cisco 安全 PIX 防火墙 VPN 故障排除需要的排错工具和技术。
- 第 9 章，“为远程接入配置 Cisco VPN 3000 应用预共享密钥”——本章介绍了如何使用预共享密钥在 Cisco VPN 3000 集中器上配置远程接入 VPN。
- 第 10 章，“为远程接入配置 Cisco VPN 3000 应用数字证书”——本章介绍了如何使用数字证书在 Cisco VPN 3000 集中器上配置远程接入 VPN。
- 第 11 章，“Cisco VPN 3000 远程接入网络的监控与管理”——本章介绍了 Cisco VPN3000 远程接入网络的监控和管理。
- 第 12 章，“扩展 Cisco IPSec 虚拟专用网络”——本章在前面章节的基础上着重介绍了 IPSec VPN 中的扩展性解决方案。

附录 A 给出了每章后面所附问题的答案。

命令语法惯例

本书中的命令语法遵循如下惯例：

- 命令、关键词和参数的实际值使用粗体字。
- 参数(需要用实际值替换)使用斜体字。
- 任选关键字和参数放在方括弧[ ]中。
- 必需的关键字和参数的选择项放在大括弧{}中。

注意：这些惯例只用于命令句法。实际配置和例子并不遵循这些惯例。

序

2001 年 1 月，Cisco Systems 公司发布了一套新的专业技术认证，即 Cisco 认证专家（Cisco Qualified Specialist，CQS）。首先推出的是 Cisco 安全专家 1（Cisco Security Specialist 1，CSS1）。CSS1 是设计用于认证技术人员的通用网络安全技能和知识，它主要集中在入侵检测系统、防火墙和虚拟专用网络。现在，业界对合格的网络安全专家的需求非常大。每天都有很多机构发现他们陷身于一场永不停息的战斗中：保护他们的网络和系统免于被蓄意破坏或者被非授权使用。对于负责检测和防范在网络中发生非授权访问或活动的网络安全专业技术人员来说，入侵检测被认为是一项关键的技能。

《Cisco 安全虚拟专用网络》（Cisco Secure Virtual Private Networks）以书籍的形式提供与本书同名的教师授课或电子教学的课程中的知识。尽管以书籍的形式来推广这些知识与参加由 Cisco 教学伙伴提供的 Cisco 认证培训中获得的动手经验不能相提并论，但它是满足全球对 Cisco 培训需求的一个极具价值的构成部分。本书将让读者能够描述、配置、验证和管理 Cisco VPN 3000 产品系列、PIX 防火墙和 Cisco 路由器中的 IPSec 特性。读者将学会如何为远程接入和场点到场点的应用来配置和管理 VPN。CSVPN 课程和本书都是致力于提供最高标准的质量和知识传递。无论读者是想完成 CSS1 认证还是对 Cisco VPN 的安装、配置和操作感兴趣，本书都将加深您对虚拟专用网络的理解。

这是为了网络安全专业技术人员事业上的成功而致力于传授网络安全知识和技能的 Cisco Press 系列丛书中的又一本新书。其他支持 CSS1 认证的图书包括：《管理 Cisco 网络安全》（Managing Cisco Network Security）、《Cisco 安全 PIX 防火墙》

（Cisco Secure PIX Firewall）和《Cisco 安全入侵检测系统》（Cisco Secure Intrusion detection Systems）。

Rick Stiffler
Cisco Systems 公司
虚拟专用网络与安全培训部经理
2001 年 9 月

致谢

在写作本书的过程中，我有幸和一组非常专业的同事们一起工作。我要感谢 Cisco Press 的 Brett Bartow，始终全力工作并保持着积极的工作态度。我也要感谢 Cisco Press 的 Drew Cupp，他对细节的严谨态度、渊博的知识和深厚的语言功底对我的帮助很大。我也要感谢 Cisco Press 项目组的其他同仁，以及本课程的最初开发者：Bob Eckhoff, Steven D. Hanna, Leon Katcharian 和 Mike Westrom，是他们的帮助才完成了本书的出版。

还要感谢技术审稿人 Kelly McGrew 和我的好友 Mark J.Newcomb，他们的技术知识和建设性意见将使我受益终生。

目　录

第一部分　虚拟专用网络（VPN）基础

第二部分 Cisco VPN 产品系统

第三部分 利用 Cisco IOS 组建 VPN

第四部分 利用 Cisco PIX 防火墙组建 VPN

第五部分　利用 Cisco VPN 集中器组建 VPN