Cisco Systems

Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com

CCSP 自学指南：Cisco 安全 PIX 防火墙 (CSPFA)

(第二版)

CCSP Self-Study:

Cisco Secure PIX Firewall Advanced (CSPFA)

Second Edition

Cisco authorized self-study book for
CCSP® 642-521 foundation learning

[美] Behzad Behtash 著
孙国冉，CCIE #12210 译
王艳奇，CCIE #12283

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

CCSP 自学指南：Cisco 安全 PIX 防火墙（CSPFA）（第二版）

[美] Behzad Behtash 著

孙国冉，CCIE #12210

王艳奇，CCIE #12283 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

CCSP 自学指南. Cisco 安全 PIX 防火墙（CSPFA）：第 2 版 /（美）贝塔什（Behtash，B.）著；孙国冉，王艳奇译. —北京：人民邮电出版社，2005.4
（Cisco 职业认证培训系列）
ISBN 7-115-13167-8

Ⅰ. C… Ⅱ. ①贝…②孙…③王… 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（2005）第 017832 号

Cisco 职业认证培训系列
CCSP 自学指南：
Cisco 安全 PIX 防火墙（CSPFA）（第二版）

◆ 著 [美] Behzad Behtash
译 孙国冉，CCIE#12210 王艳奇，CCIE#12283
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 010-67132692
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：41
字数：1 000 千字 2005 年 4 月第 1 版
印数：1－3 500 册 2005 年 4 月北京第 1 次印刷

著作权合同登记 图字：01-2004-0564 号
ISBN 7-115-13167-8/TP・4497

定价：88.00 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

本书分 7 个部分对 Cisco 公司网络安全的拳头产品 PIX 防火墙进行了系统讲述。第 1 部分讲述了网络安全的基础知识、实施安全策略的基本方法、Cisco 公司网络安全方面的产品概况，并对 PIX 防火墙的各种型号和基本特点进行了系统阐述。第 2 部分通过举例的方式讲述了在不同规模和不同复杂程度的环境下部署 PIX 防火墙的具体方法和配置。第 3 部分对 PIX 防火墙的配置进行了详细讲解，包括基本配置、PDM 管理配置、地址和端口转换配置、访问控制列表和内容过滤的配置、为简化配置如何进行对象分组、基本的路由配置。第 4 部分讲述的是高级配置，包括如何配置 PIX 防火墙以支持特殊的上层协议和多媒体协议，如何配置攻击保护、入侵检测和动态阻挡，如何配置认证、授权和记帐，如何配置故障倒换以提高安全系统的可靠性。第 5 部分对 VPN 中的关键技术，如 IPSec 进行了概要的描述，然后讲述了使用 PIX 防火墙构建不同类型的 VPN 时的具体配置方法。第 6 部分讲述的是 PIX 防火墙的维护和管理，特别是在企业网中如何使用防火墙管理中心（MC）和 AUS 以图形化的方式管理和维护防火墙。第 7 部分则以专题的方式分别讲述了专用 Cisco 6500 交换机和 Cisco 7600 路由器上的防火墙服务模块（FWSM）、使用 SOHO 网络的 PIX 防火墙。

本书讲述的重点是如何在实际环境中应用 PIX 防火墙，所以关注的不是某项技术的细节，而是产品应用时的各种配置。本书适合于准备进行 CCSP 认证考试的考生，也适合于想对 PIX 防火墙的应用有深入了解的各类工程技术人员。

关于作者

Behzad Behtash，CCNP，CCDP，MCSE，是一名 IT 顾问，在组网和安全方面有 9 年多的经验，拥有威斯康星——麦迪逊大学化学工程专业的学士学位，居住在加利福尼亚的奥克兰。

关于技术审稿人

Nairi Adamian，CCIE Security No.10294，CISSP，工作在位于澳大利亚的 Cisco 系统公司技术支持中心（TAC），是一名负责安全和虚拟专用网（VPN）的工程师。她为 Cisco 多种安全产品提供技术支持，如 PIX 防火墙、VPN 集中器、入侵监测系统以及其他相关的技术，拥有悉尼理工大学计算机科学专业的学士学位，目前正在攻读 Macquarie 研究生管理学院的 MBA。

Andy Fox，CCNA，CCDA，CSS-1，是 Global Knowledge 公司 Cisco 认证的一名讲师。Andy 讲解 Cisco 的认证课程已有 6 年多，是“管理 Cisco 网络安全”课程方面的主管，是本书（《Cisco 安全 PIX 防火墙》）第一版的作者。Andy 在美国空军时是一名计算机操作员，从那时起开始从事计算机科学相关工作。

Izak Karmona 是 HP 公司的网络安全顾问，工作在以色列，是一名 CCSP，目前正在努力获取 CCIE 安全证书。Izak 在网络行业工作超过了 15 年。他的工作包括为 HP 公司的客户提供网络设计、安全和实施服务。Izak 拥有以色列海尔法理工学院（Technion Institue of Technology）计算机科学专业的学士学位。

献　辞

把这本书献给我的女儿 Tiana；我的儿子 Daryan；还有我亲爱的妻子 Anita，她总是我的第一个读者。

另外，我也把这本书献给我的父母，感谢他们对我无私的关爱和支持。同时献给 Ramin、Kaveh 和 Saman，亲爱的哥哥和朋友。

我还要感谢另外两个值得尊敬的人，他们对我的成长帮助甚多：威斯康星——麦迪逊大学的 Glenn Sather 和 Thatcher Root 教授。谢谢他们对我的信任。

致　谢

我要感谢 Michelle Grandin，Christopher Cleveland，Tammi Barnett，Kris Simmons，San Dee Phillips，Keith Clien，以及其他 Cisco Press 的同仁，感谢他们给我写这本书的机会，感谢他们在本书整个写作过程中所给与的支持和指导。特别感谢 Betsey Henkels，一位非常好的合作者。她是一名资深的技术人员，作为本书的开发编辑，她所付出的努力使本书的质量大为提高。

我还要感谢审稿人 Nairi Adamian、Andy Fox 和 Izak Karmona，感谢他们的贡献和建设性的建议。他们的奉献，让我十分感激。

我还要感谢我的大学同学和朋友 Grant Moerschel，是他把我介绍给 Cisco Press，感谢他的友谊和洞察力。

最后，我要感谢在 Cisco 系统公司工作的 Matt Krieg，感谢他提供了有关 PIX 防火墙开发方面的及时信息。

序　言

本书是Cisco Systems公司认可的学习教材，可以帮助你理解Cisco 安全防火墙高级（CSPFA）考试中所涉及的概念。本书是和Cisco Internet学习解决方案小组合作开发的，这个团队在Cisco Systems公司负责开发CSPFA考试。作为考前辅导教材，本书详细、全面地阐述了一个网络和安全工程师配置、验证和管理PIX防火墙系列产品的方方面面。无论你要通过CCSP的认证，还是要成为PIX专业人士，或者只是想更好地理解产品、服务和策略，以便应用PIX防火墙系列中的产品，这本书都能让你从中获益。

Cisco Systems公司和Cisco Press提供本书的印刷版本，旨在让客户和广大用户能够以另一种方式进行学习。虽然出版物不同于教师指导环境和远程学习环境，但毕竟学习方式因人而异。通过Cisco Press出版本书，旨在将知识传播给更多的网络专业人员。

Cisco Press将针对已有的和将推出的考试，出版其他认证自学系列丛书，帮助Cisco Internet学习解决方案小组实现其首要目标：对Cisco网络技术领域的专业人员进行培训，使其能够组建和维护可靠的、易于扩展的网络。Cisco职业认证和相应的课程通过严谨、循序渐进的培训来实现上述目标。

为通过Cisco职业认证并完成Cisco认证的专业人员的日常工作，建议结合采用教师指导的培训、实际动手、远程学习、自学等学习方式。Cisco Systems授权的培训合作伙伴遍布世界各地，他们提供高质量的指导以及宝贵的实验室和模拟环境。有关当地的Cisco培训伙伴计划的详细，请访问http://www.cisco.com/go/authorizedtraining。

Cisco Press和Cisco Systems合作出版的书籍符合相应课程和认证的质量要求。希望本书以及后续的认证自学图书对增强读者的网络知识大有裨益。

Thomas M. Kelly
Cisco Systems公司
Cisco Internet学习解决方案分部副总裁
2004年1月

前　言

过去几年里，网络安全引起了越来越多的关注。当前的环境和对安全的普遍关注增强了人们对网络安全技术和产品的重视。这一点直接反映在对网络安全产品和服务投资的增加上，也反映在对网络安全专业人员和安全专家的需求不断增加上。

为适应市场对安全的需要，Cisco Systems 公司提供了多种网络安全产品、创新的技术和服务。Cisco PIX 防火墙安全系列产品是占据主导市场份额的防火墙产品，众多的网络工程师和专业的安全人士用它们为各种规模和复杂程度的网络提供保护。

读者对象

本书的读者是需要了解有关 PIX 防火墙安装、配置和维护详细信息的网络工程师、安全专业人员和支持工程师。准备参加 CCSP 考试的人员也可以用它作为考前的辅导教材。要充分理解本书的信息，读者应该具有扎实的网络基础知识，熟悉网络安全的基本概念。

本书的初衷

Cisco Press 于 2001 年发行了《Cisco 安全 PIX 防火墙》的第一版，书中讲述了 PIX 防火墙的操作和高级特性，满足了当时市场的需求。从出版第一版以后，PIX 防火墙已经进行了重大的改进和提高，引入了几种新的型号，包括针对 Cisco 6500 系列交换机和 Cisco 7600 系列 Internet 路由器的模块。Cisco 系统公司还引入了使用图形化用户界面的 PIX 设备管理器（PDM），改善了对企业网中 PIX 防火墙的维护和管理。

本书包含了 CSPFA 第一版出版以后的更新信息、新引入的 PIX 防火墙型号和技术。其中包括 PIX 防火墙软件版本 6.3 中引入的开放式最短路径优先协议（OSPF）、802.1Q VLAN 和逻辑接口、网络地址转换（NAT）遍历。另外，更多的重点放在了 PDM 上，它将是管理和配置 PIX 防火墙最主要的工具。

如何使用本书

本书共包括 22 章，这些章节是按照逻辑顺序进行排列的，不过你可以按照自己的需要方便地阅读任何章节。第 4 章中举了几个例子，通过它们你可以了解网络的典型布局并完成 PIX 防火墙的配置。你可以参照这章的内容确定实施中基本的网络布局，在此基础上学习后续的章节。当然，你也可以在读过了其他章节以后再来阅读第 4 章，你将发现对这一章的内容已经非常熟悉。

各章的内容如下。

第 1 章，“Cisco 网络安全方面的产品”——这一章对网络安全进行了概述，并简要地描述了 Cisco 语音、视频与集成数据架构（AVVID）和企业网安全架构（SAFE）的框架。

第 2 章，“Cisco PIX 防火墙技术与特点”——这一章对 PIX 防火墙技术和能力进行了简要描述，其中介绍了适应性安全算法（ASA）。

第 3 章，“Cisco PIX 防火墙系列产品介绍”——这一章讲述了 PIX 防火墙安全产品系列，介绍了各种型号产品的特点和功能。

第 4 章，“在网络中实施 Cisco PIX 防火墙”——这一章举例说明了在不同规模和复杂程度的网络中，如何实施 PIX 防火墙。

第 5 章，“Cisco PIX 防火墙入门”——这一章讲述了 PDM 的操作，以及使用 PDM 配置 PIX 防火墙的步骤。

第 6 章，“Cisco PIX 设备管理器”——这一章介绍 PDM 操作以及使用 PDM 配置 PIX 防火墙的过程。

第 7 章，“转换和连接”——这一章详细说明了 PIX 防火墙如何处理入站和出站数据，还讲述了网络地址转换（NAT）和端口地址转换（PAT）技术。

第 8 章，“访问控制列表和内容过滤”——这一章讲述了如何使用访问控制列表（ACL）来控制穿过 PIX 防火墙的数据流。

第 9 章，“对象分组”——这一章讲述了 PIX 防火墙的对象分组功能，通过这项功能来简化创建和应用 ACL 的步骤。

第 10 章，“路由选择”——这一章讲述了 PIX 防火墙支持的路由选择功能。

第 11 章，“高级协议处理”——这一章讲述了 PIX 防火墙的协议修正功能以及高级协议处理能力。

第 12 章，“攻击保护、入侵检测和动态阻挡”——这一章讲述了 PIX 防火墙的在线入侵检测和动态阻挡功能，以及相关的配置步骤。

第 13 章，“认证、授权和记帐”——这一章简要介绍了 PIX 防火墙认证、授权和记帐（AAA）的步骤，还讨论了可下载的 ACL。

第 14 章，“故障倒换”——这一章详细介绍 PIX 防火墙的高可用性和相关的配置步骤。

第 15 章，“虚拟专用网”——这一章简要讲述了 VPN 的基础知识，以及如何在 PIX 防

火墙中实施 IP 安全（IPSec）和 Internet 密钥交换（IKE）。

第 16 章，“站到站 VPN”——这一章详细讲述了使用 PIX 防火墙构建站到站 VPN 连接的配置步骤。

第 17 章，“客户远程访问 VPN”——这一章详细讲述了使用 PIX 防火墙构建客户远程访问 VPN 连接的步骤。

第 18 章，“系统维护”——这一章详细讲述了 PIX 防火墙的系统维护协议和配置任务，包括映像更新和密码恢复步骤。

第 19 章，“企业网中的 PIX 防火墙管理”——这一章讲述了 Cisco 防火墙管理中心（防火墙 MC）的操作和功能。

第 20 章，“企业网中的 PIX 防火墙维护”——这一章讲述了如何使用防火墙自动升级服务器来维护企业网中 PIX 防火墙的运行。

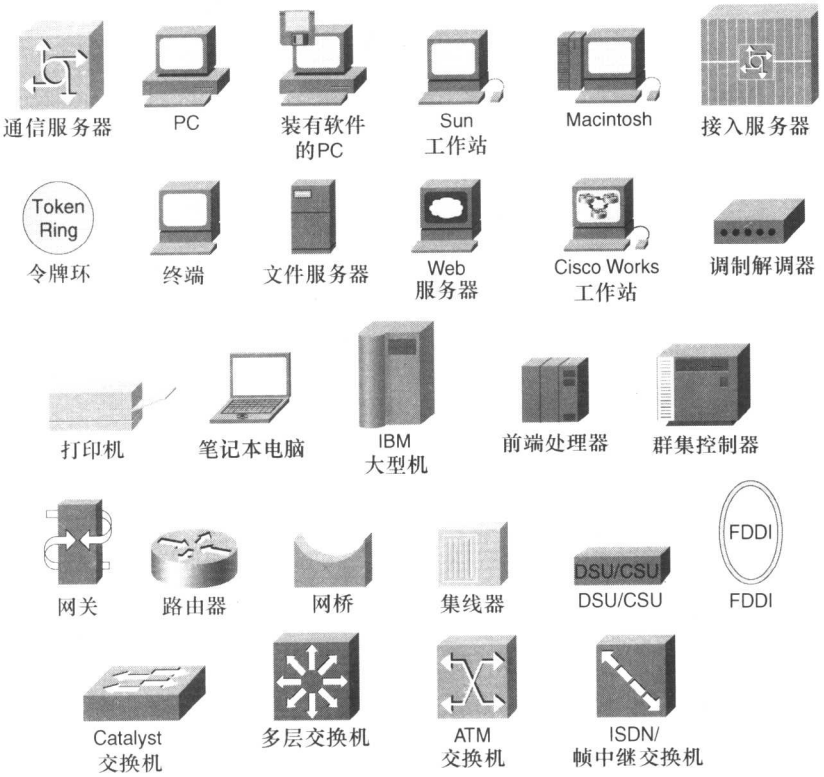
第 21 章，“防火墙服务模块”——这一章详细讲述了用于 Cisco Catalyst 6500 系列交换机和 Csico 7600 系列 Internet 路由器上的 PIX 防火墙服务模块（FWSM）的功能。

第 22 章，“SOHO 网络中的 PIX 防火墙”——这一章重点讲述了 PIX 防火墙针对小办公室/家庭办公室（SOHO）网络的功能和技术。

附录 A，“复习题答案”——这个附录是各章复习题的答案。

附录 B，“安全资源”——这个附录列举了很多有用的安全资源，包括书籍和 Internet 上的资源。

本书使用的图标



网络云图 实线：以太网 折线：串行电路 虚线：交换式串行连接

命令语法规范

本书使用的命令语法规范和IOS命令参考中使用的规范是一样的。命令参考中对规范的描述如下。

- **粗体**表示要逐个字符键入的命令和关键字。在实际配置举例和输出中（不是在通用命令语法中），**粗体**表示由用户手工输入（比如**show**命令）的内容。
- *斜体字*表示的是参数，在实际使用时需要用实际值来替代。
- 垂直线（|）把多个选项分隔开，只能选择其中的一个。
- 方括号[]表示可选元素。
- 大括号{}表示必选项。
- 位于方括号中的（[{}]）表示可选元素中的必选项。

目　录

第一部分　概　述

第五部分 VPN 配置