



Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com



CCSP Cisco 安全 PIX 防火墙 (CSPFA)认证考试指南 (第二版)

CCSP™ Self-Study

CCSP Cisco Secure PIX® Firewall Advanced

Exam Certification Guide

Second Edition

Official self-study test preparation guide for the
Cisco CSPFA 642-521 exam

内附光盘



[美] Greg Bastien
Earl Carter 著
Christian Abera Degu
高和生 孙利民 赵军锁 译

 人民邮电出版社
POSTS & TELECOM PRESS

Cisco 职业认证培训系列

CCSP Cisco 安全 PIX 防火墙 (CSPFA) 认证考试指南 (第二版)

Greg Bastien
[美] Earl Carter 著
Christian Abera Degu

高和生 孙利民 赵军锁 译

人民邮电出版社

图书在版编目 (CIP) 数据

CCSP Cisco 安全 PIX 防火墙 (CSPFA) 认证考试指南: 第 2 版 / (美) 巴斯琴 (Bastien, G.), (美) 德古 (Degu, C. A.) 著; 孙利民, 赵军锁译. —北京: 人民邮电出版社, 2005.7

ISBN 7-115-13486-3

I. C... II. ①巴...②德...③孙...④赵... III. 计算机网络—防火墙—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 060454 号

版 权 声 明

Greg Bastien Earl Carter Christian Abera Degu: CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide Second Edition.

Copyright ©2005 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 PIX 防火墙 (CSPFA) 认证考试指南 (第二版)

-
- ◆ 著 [美] Greg Bastien Earl Carter Christian Abera Degu
译 高和生 孙利民 赵军锁
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>
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: 31.75
字数: 771 千字 2005 年 7 月第 1 版
印数: 1~3 500 册 2005 年 7 月北京第 1 次印刷

著作权合同登记 图字: 01-2005-0795 号

ISBN 7-115-13486-3/TP · 4701

定价: 78.00 元 (附光盘)

读者服务热线: (010) 67132705 印装质量热线: (010) 67129223

内容提要

本书是通过 Cisco PIX 防火墙认证考试(CSPFA 642-521)的官方认证考试指南。全书共分为 20 章,分别介绍了网络安全、防火墙技术和 Cisco PIX 防火墙、Cisco PIX 防火墙、系统管理/维护、理解 Cisco PIX 防火墙转换和连接、开始使用 Cisco PIX 防火墙、配置访问、系统日志、路由和 PIX 防火墙、Cisco PIX 防火墙故障切换、虚拟专用网、配置访问 VPN、PIX 设备管理器、CiscoWorks 防火墙管理中心 (PIX MC)、PIX 上的内容过滤、AAA 和 Cisco PIX 防火墙概述、Cisco PIX 防火墙上的 AAA 配置、攻击防护和高级协议处理、防火墙服务模块、案例研究和配置示例。附录提供了各章模拟试题的答案。

本书适合于准备参加 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

Greg Bastien: CCNP、CCSP、CISSP, 现在是 Virtue 技术有限公司的技术主管。他为许多联邦机构和商业客户提供咨询服务, 并在 Strayer 大学担任兼职教授, 讲授网络和网络安全教程。他在美国军队担任直升机飞行教官期间, 完成了在 Embry-Riddle 航空大学的本科和研究生学位。

Earl Carter: CCNA, 已经在计算机安全领域工作了 8 年。他在空军信息作战中心工作开始学习计算机安全方面的知识, 主要负责保护空军网络免受攻击。1998 年他到 Cisco Systems 公司工作, 为 NetRanger(现在 Cisco IDS)和 NetSonar (Cisco Secure Scanner) 进行入侵检测系统 (IDS) 研究。Earl 花费了大约一年为 NetRanger 编写签名, 为 NetSonar 开发软件模块。现在他是咨询工程 (CE) 下属的安全技术诊断小组 (STAT) 的成员, 负责对 Cisco 产品进行安全评估, 并与 Cisco 的其他小组一起帮助提高 Cisco 产品的安全性。他已经检查了从 PIX 防火墙到 Cisco CallManager 等多个产品。现在, Earl 正在为以安全为重点的 CCIE 证书而努力。

Christian Degu: CCNP、CCDP、CCSP, 现在, 是从事通用动态网络系统信号解决方案工作的高级网络工程师, 也是联邦能源管理委员会的一名咨询工程师。他是计算机信息系统的硕士, 现居住在 Virginia 州的 Alexandria。

关于技术审稿人

Behzad Behtash 是一位有 10 多年网络经验, 尤其是有线和无线网络安全方面经验的 IT 咨询专家。Behzad 拥有 Madison 的 Wisconsin 大学的化学工程学士学位, 现居住在 California 的 Oakland。他获得了 CCNP、CCDP、CCSP 和 MSCE 证书, 并是本书配套教材的作者。

Izak Karmona: CCSP、CCNA、CSS-1, 是以色列的一名网络安全顾问, 现在正在备考 CCIE 安全证书。Izak 在网络方面具有 15 年以上的工作经验。作为工作的一部分, 他为客户提供网络设计、安全和实现服务。Izak 拥有以色列 Haifa 市的 Technion 工学院的计算机科学学士学位。

Tim Sammut: CCIE No.6642, 是 Northrop Grumman 信息技术公司的高级网络咨询专家。他参加了许多重大项目, 涉及 LAN 交换技术、SNA 集成的安全等内容, 还帮助许多组织构建网络。他还获得了 CISSP、CCIE 安全和 CCIE 服务提供商证书。

献

辞

献给 Ingrid、Joshua、Lukas 和我在 Virtue 技术公司的朋友，尤其是 Todd Schweitzer 和 Meti Gizaw。感谢你们在整个项目中对我的支持。

——Greg Bastien

没有亲爱的家人，就没有我的今天。他们一直都在支持我的工作。因此，我将本书献给我的妻子 Chris、我的女儿 Ariel 和我的儿子 Aidan。

——Earl Carter

献给 Meron Tamrat Desta，感谢你的爱和一直对我的支持。

——Christian Degu

致

谢

Greg Bastien: 网络安全无疑是一个快速发展的市场，跟上它的变化需要持续不断的努力。我们要感谢 Cisco Press 的工作人员，感谢他们使我们能及时追踪发展潮流。还要特别感谢组稿编辑 Michelle Grandin、高级开发编辑 Chris Cleveland 和开发编辑 Howard Jones，感谢他们的努力工作。

Earl Carter: 首先，我想说在本书的写作中有许多人帮助了我（太多以至于无法一一列出来）。我所接触的每个人都非常支持和合作，感谢你们的帮助。我还想感谢 Mr.和 Mrs.Nowakowski 对我在 Taekwondo 和其他工作中的鼓励。最后，我想感谢 Jesus Christ 在我生命中给予的恩惠，在写作的漫长日子（经常到深夜）里给予我帮助的温暖家庭。

本书使用的图标

在本书中你可以看到用于网络设备的下列图标：



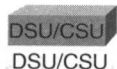
路由器



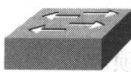
网桥



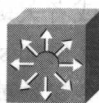
集线器



DSU/CSU



Catalyst
交换机



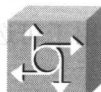
多层交换机



ATM
交换机



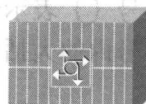
ISDN/帧中继
交换机



通信服务器



网关



接入服务器



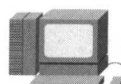
PC



带软件的 PC



Sun 工作站



Macintosh



终端



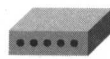
文件服务器



Web 工作站



Cisco Works
工作站



调制解调器



打印机



膝上电脑



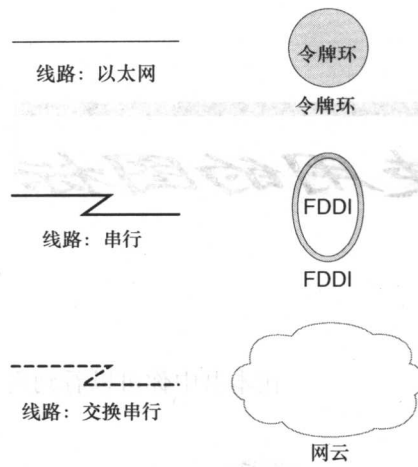
IBM 主机



前端处理器



簇控制器



本书中使用的约定

本书中用于表示命令语法的习惯与用于 IOS 命令参考中的相同。具体说明如下：

- **黑体**表示用户逐字键入的命令或者关键字。在实际配置例子和输出（不是命令语法）中，黑体表示用户手工输入的命令（例如 **show** 命令）。
- *斜体*表示用户提供值的一个命令参数或者选项。
- 垂直线（|）表示分隔备选项、相互排斥的命令选项。
- 方括号 [] 表示命令的一个任选元素。
- 大括号 { } 表示命令必需的选项。
- 方括号内的大括号（ [{ }] ）表示用于可选项内的必选项。

前 言

本书是帮你通过 Cisco 安全 PIX 防火墙高级认证考试 (CSPFA 642-521) 的辅助工具。

为什么出第二版?

网络安全是急剧动态变化的。每天都有新的威胁,而且新技术和新产品几乎以同样的速度不断投入市场。《CCSP Cisco 安全 PIX 防火墙认证考试指南》第一版出版 4 个月后, Cisco 系统公司完成了 PIX 6.3 (1) 版,并更新了证书考试以反映新版本中增加的功能。本书是依据 PIX 6.3 (3) 版而写的,我们不能预计 PIX 操作系统在近期的任何主要版本变化。

谁应该读这本书

网络安全是一个非常复杂的问题。Cisco PIX 防火墙作为安全程序的一部分执行了一些非常特殊的功能。在你着手 CSPFA 认证之前,熟悉许多网络和网络安全概念非常重要。本书是为那些开始对安全认证过程感兴趣的安全专业人员和网络专业人员设计的。

如何使用本书

本书由 20 章组成,每一章都以前一章为基础。涉及特殊命令和配置的章节都包括案例研究 (case study) 或者配置示例。第 20 章包括了附加的案例研究和配置示例——可能是对的也可能不对——它能够让你决定配置是否能够满足要求,以及为什么能够满足要求。

写作本书的主要目的是帮助读者准备 CSPFA 认证考试。它只是一个工具,而不是完整的“工具箱”。也就是说,你还需要配合其他的参考资料 (尤其是 Cisco TAC) 来准备考试。记住,成功通过考试只是一个伟大的短期目标,精通你做的事情才是你永远的目标。

本书各章所涉及的知识点如下:

- **第 1 章，“网络安全”**——本章提供了网络安全的一个概述——网络安全过程和潜在的威胁。也讨论了在公司关系变得越来越密切，并且他们的网络边界变得越来越模糊时，网络安全如何对商务变得日益重要。本章还讨论了网络安全策略和两个 Cisco 程序，它们能够帮助公司设计和实现可靠的安全策略、过程和体系结构。
- **第 2 章，“防火墙技术和 Cisco PIX 防火墙”**——本章涉及了不同的防火墙技术和 Cisco PIX 防火墙。本章分析了 PIX 防火墙的设计并且讨论了这些设计的一些安全优势。
- **第 3 章，“Cisco PIX 防火墙”**——本章更详细地讨论了 Cisco PIX 防火墙的设计，还列出了不同的 PIX 型号和它们的应用目标，并讨论了每种型号各种可用的特性以及它们是如何实现的。
- **第 4 章，“系统管理/维护”**——本章详细讨论了 Cisco PIX 防火墙 IOS 的安装和配置。本章涉及允许 PIX 远程管理的不同配置选项。
- **第 5 章，“理解 Cisco PIX 防火墙的转换和连接”**——本章涉及不同的转换协议以及 PIX 防火墙 IOS 是如何处理它们的。本章也讨论了网络地址和 PIX 如何能够更改节点或者网络地址，以确保这些要素的安全。
- **第 6 章，“开始使用 Cisco PIX 防火墙”**——从本章才开始真正接触到 PIX 的“骨肉”。本章涉及 PIX 操作的基本命令，讨论了连接 PIX 防火墙的方法以及 PIX 可用的众多配置选项中的一部分。
- **第 7 章，“配置访问”**——本章涉及允许对使用 PIX 防火墙的网络控制访问的不同配置。本章也涉及允许特定协议通过防火墙所需要的一些特殊配置。
- **第 8 章，“系统日志和 PIX”**——本章涉及 PIX 防火墙日志功能，以及允许 PIX 防火墙登录一个系统日志服务器所需要的配置。
- **第 9 章，“路由选择和 PIX 防火墙”**——本章讲述了 PIX 防火墙的路由、PIX 支持的路由协议及如何实现它们。
- **第 10 章，“Cisco PIX 防火墙故障切换”**——本章讨论一个冗余防火墙配置的好处，以及在故障切换模式下配置两个 PIX 防火墙所需要的步骤。
- **第 11 章，“虚拟专用网”**——许多的商业活动处于不同的位置，它们需要相互连接。本章研究了能够配置在 PIX 防火墙和其他 VPN 端点间的虚拟专用网安全连接的不同类型。它涉及用于穿过公共网络创建和维护 VPN 的技术和协议。
- **第 12 章，“配置访问 VPN”**——本章讨论了如何使用 PIX 防火墙来创建远程访问虚拟专用网。
- **第 13 章，“PIX 设备管理器”**——能够使用多种工具管理 Cisco PIX 防火墙。PIX 设备管理器是一个能够用于管理 PIX 的基于 Web 的图形用户接口（GUI）。
- **第 14 章，“CiscoWorks 防火墙管理中心（PIX MC）”**——CiscoWorks 是为在一个企业环境中管理多个 Cisco 产品而开发的工具。本章概述了 CiscoWorks，并讨论了 PIX MC 的用于管理 PIX 防火墙的部件。
- **第 15 章，“用 PIX 防火墙进行内容过滤”**——将攻击代码置入到一个 Web 页中是黑客常用的手法。某些类型的程序代码因为它们的交互特性特别适合这种类型的攻击。本章讨论这些类型的代码并确定它们的危险性。
- **第 16 章，“AAA 和 PIX 防火墙概述”**——确保只有授权的用户才能访问你的网络

极其重要。本章讨论了配置认证、授权和统计 (AAA) 服务的 PIX 防火墙的不同方法。还介绍了 Cisco 安全访问控制服务器 (CSACS)，它是 Cisco 的 AAA 服务器包。

- **第 17 章，“在 PIX 防火墙上配置 AAA”**——本章讨论了与 AAA 服务器通信而在 PIX 防火墙上的特殊配置，包括 CSACS。涉及了 PIX 防火墙上 AAA 的实现、功能和疑难解析。
- **第 18 章，“攻击防护和高级协议处理”**——许多不同类型的攻击是针对网络和它的周边设备发动的。本章讨论了大部分常见的攻击，以及怎样配置 PIX 防火墙来抵制这些攻击。
- **第 19 章，“防火墙服务模块”**——本章详细讲述了 PIX 防火墙服务模块 (FWSM)，它是 Catalyst 6000 系列交换机设计的关键模块。FWSM 为核心交换基础设施提供了防火墙功能。
- **第 20 章，“案例研究和配置示例”**——本章由两个案例组成，使读者能够实践配置防火墙以执行特定的功能。一部分包括可能对也可能不对的配置。这要求读者确定配置是否能够正确工作，原因是什么。认证考试会问关于 PIX 防火墙配置的特定问题。熟悉 PIX 防火墙配置的不同命令和部件对考试非常重要。

本书中每章都有相同的格式，通过对你当前知识的评估和强调本章使你感兴趣的特殊领域来辅导你。

- **“我已经知道了吗？”测验**——每章的开始都有一个测试，帮助你评估对本章知识的掌握情况。这个测试主要涉及所强调的特定领域，从而帮助你选择应该着重学习这一章中的哪些内容。
- **基础内容**——这是每章的核心部分。它主要讲述为成功地准备考试而必须熟练掌握的特定协议、概念或者技巧。
- **基础总结**——在每章的结尾，都要将本章的基础内容总结成重点集锦。在大部分情况下，基础内容总结在图表中。但在有些情况下，每章中的重点部分只在问题范围内简单地重申一下以强调它们的重要性。记住本书中每章的基础内容部分只能帮助读者评估对考试的准备情况。虽然基础内容和基础总结是你在考试前最后时刻复习的好工具，但是只学习这些就能成功地完成考试是不太可能的。
- **问答题**——每一章的结尾都列有一些复习题，它们可以考察读者对学习内容的理解程度。回答这些问题不仅是确保读者理解学习内容的好方法，而且是锻炼处理实际问题的能力最好方法。
- **案例研究/场景**——这一章更多的是讨论在简单场景中配置 Cisco PIX 防火墙。这些场景能够帮助你理解不同的配置选项，以及在防火墙的配置中每个组件是如何影响其他组件的。本书将要结束时的两个案例研究允许你练习配置防火墙执行特定的功能。
- **CD 上的测试题**——在本书所附的 CD 上，你会发现有超过 200 个题目的测试题，这些问题覆盖了 CSPFA 考试的重点。使用我们可定制的考试引擎，你就能设计一个测试用例，它或者是集中于特定的问题领域，或者是一些随机的题目。每个测试题目有一个指向本书电子 PDF 版的相关部分的链接，它也包含在 CD 上。

图 I-1 给出了浏览本书的最佳方法。如果你感到已经充分理解了某一章中的内容，你可

以通过“我已经知道了吗？”测验对自己进行测试。根据所得分数，可以决定是学习整章还是跳到“基础总结”和“问答题”部分。推荐读者阅读整本书，而不是跳着读。毕竟一个人不可能对一个主题知道太多。只有当你参加了考试，才可能知道你是否真正掌握了每个主题，但那时已经太晚了。

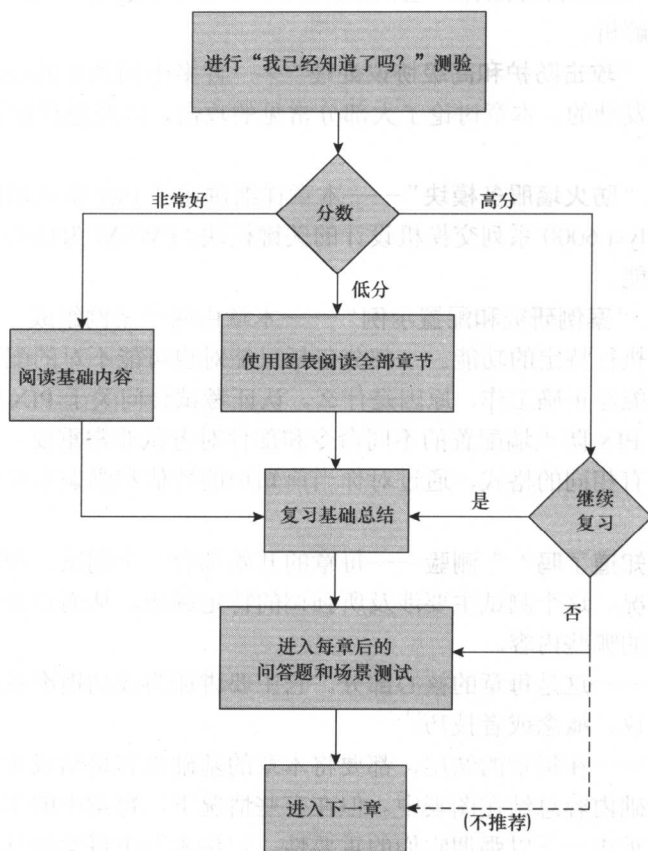


图 I-1 阅读每章内容

认证考试和这本备考指南

每个认证考试的题目都会极其保密。就算你得到了这些题目并且通过了考试，一旦开始第一个需要 PIX 技巧的工作时，你也会遇到许多困难。也就是说要精通这些资料，而不仅仅是成功地通过考试。我们知道什么问题是通过这个考试所必须理解的，巧合的是，这些问题也是熟练掌握 PIX 防火墙所需要的。我们将这些问题分成“基础内容”并且将它们贯穿于本书的始末。表 I-1 描述了每一项基础内容。

表 I-1

CSPFA 基础知识点和描述

参考号	考点	描述
1	防火墙	防火墙以 3 种不同的方法处理网络流量。第 2 章讨论了这些技术和它们的优点
2	PIX 防火墙型号	目前 PIX 防火墙有 6 种不同的型号。第 3 章讨论了每种型号、它们的技术条件以及如何和什么时候应用它们

续表

参考号	考点	描述
3	PIX 服务模块	PIX 防火墙服务模块 (FWSM) 是为 Catalyst 6000 系列交换机提供 PIX 防火墙功能的关键。该部件在第 19 章中讨论
4	PIX 防火墙许可	第 3 章讨论了 PIX 防火墙可用的不同许可选项, 以及每种许可的应用
5	用户接口	CLI 是用于配置 PIX 防火墙的一种方法。第 6 章涉及 CLI 和用于配置防火墙的许多命令
6	检验 PIX 防火墙状态	认证 PIX 防火墙配置能够帮助你查找连通性的问题。疑难解析将作为本书中每个任务的一部分进行讨论
7	ASA 安全等级	自适应安全算法 (ASA) 是 PIX 防火墙的一个关键组件。在第 2、第 3、第 5 和第 6 章中详细讨论这个问题
8	基本 PIX 防火墙配置	PIX 防火墙的基本配置在第 6 章中讨论
9	系统日志配置	第 8 章涉及 PIX 防火墙的日志特性
10	DHCP 服务器配置	PIX 防火墙能够配置成一个 DHCP 服务器和一个 DHCP 客户端。第 3、第 6 和第 12 章涉及了这些配置
11	PPPoE 和 PIX 防火墙	PPPoE 用于通过一个单独的拨号连接或者宽带连接来连接多台主机。一些 PIX 防火墙型号支持 PPPoE。这个问题在第 12 章中讨论
12	传输协议	传输层协议和 PIX 防火墙如何处理它们在第 5 章和第 8 章中讨论
13	网络地址转换	许多不同的防火墙使用网络地址转换以保护网段的安全。这在第 5 章和第 6 章中讨论
14	配置 DNS 支持	作为一个周边设备, PIX 防火墙必须支持域名服务。在 PIX 上配置 DNS 在第 6 章中讨论
15	端口地址转换	端口地址转换是一个 PIX 防火墙用于将 NAT 多个内部源转换到一个单独的外部地址的方法。第 5 章和第 6 章中涉及这个配置
16	ACL	访问控制列表用于允许或者拒绝通过 PIX 防火墙的不同网段间的流量。配置 ACL 在第 7 章中讨论
17	将管道转换为 ACL	管道来自预先填写 ACL 的命令集。它们试图扩展功能。第 7 章讨论管道和 ACL
18	使用 ACL	配置和使用 ACL 在第 7 章中讨论
19	对象分组概述	服务、主机和网络对象能够被防火墙分组以便更有效地处理。对象分组在第 7 章中讨论
20	开始使用组对象	对象分组在第 7 章中讨论
21	配置组对象	对象分组在第 7 章中讨论
22	嵌套对象组	对象组可能嵌套到其他的对象组中。对象分组在第 7 章中讨论
23	高级协议	许多高级协议需要防火墙的特殊处理。一些协议需要多个入站和出站的连接。PIX 防火墙处理这些高级协议在第 7 章中讨论
24	多媒体支持	多媒体协议被看成高级协议。PIX 防火墙的高级协议处理在第 7 章和第 18 章中讨论
25	攻击防护	能够配置 PIX 防火墙辨别一个攻击并对它做出反应。这在第 18 章中讨论
26	入侵检测	能够配置 PIX 防火墙作为一个入侵检测系统来运行。也能够与外部 IDS 一起工作。这些问题在第 18 章中讨论
27	AAA 概述	AAA 是一种确保能够检验谁正访问你的网络资源, 限制他们对特定资源的访问, 以及追踪他们在网络中行为的一种方法, 配置 PIX 防火墙支持 AAA 在第 16 和第 17 章中讨论
28	为 Windows NT/2000 安装 CSACS	CSACS 也是一个 Cisco AAA 服务器产品。安装和配置 CSACS 在第 17 章中讨论
29	认证配置	配置 CSACS 在第 16 章和第 17 章中讨论
30	可下载 ACL	配置 CSACS 在第 16 章和第 17 章中讨论
31	理解故障切换	关键任务系统需要高可用性的解决方案以将网络出故障的可能性降为最小。配置两个防火墙能够作为一个高可用性的方案。这个配置在第 10 章中讨论
32	串行故障切换配置	PIX 故障切换配置在第 10 章中讨论

续表

参考号	考点	描述
33	基于 LAN 的故障切换配置	PIX 故障切换配置在第 10 章中讨论
34	PIX 防火墙启用一个安全 VPN	不同位置间的专用电路可能受成本的限制,但是只在这些穿过公共网络空间的位置之间创建一个加密的连接,造价就要低得多。配置虚拟专用网在第 11 章中讨论
35	准备配置 VPN 支持	一个虚拟专用网的两端必须有一个终结点。PIX 防火墙能够配置成一个 VPN 终结点。配置虚拟专用网在第 11 章中讨论
36	配置 IKE 参数	IKE 是用于确保加密连接不容易被破解的一个关键的交换的方法。配置虚拟专用网在第 11 章中讨论
37	配置 IPSec 参数	IP 安全 (IPSec) 是创建加密 VPN 连接的一个标准。配置虚拟专用网在第 11 章中讨论
38	测试和认证 VPN 配置	虚拟专用网的配置和疑难解析在第 11 章中讨论
39	Cisco VPN 客户端	远程用户能够使用 VPN 客户端软件创建从他们的计算机到公司网络的一个 VPN。配置虚拟专用网和 VPN 客户端软件在第 12 章中讨论
40	可扩展的 PIX 防火墙 VPN	配置虚拟专用网在第 11 章中讨论
41	远程访问	能够本地或者远程管理 PIX 防火墙。配置 PIX 以允许远程访问在第 4 章中讨论
42	命令级认证	PIX 防火墙的远程管理在第 4 章中讨论
43	PDM 概述	PIX 设备管理器 (PDM) 是一个用于 PIX 防火墙远程管理的 Web 启用的工具。使用 PDM 的 PIX 远程管理在第 13 章中讨论
44	PDM 准备	PIX 设备管理器 (PDM) 是一个用于 PIX 防火墙远程管理的 Web 启用的工具。使用 PDM 的 PIX 远程管理在第 13 章中讨论
45	使用 PDM 配置 PIX 防火墙	PIX 设备管理器 (PDM) 是一个用于 PIX 防火墙远程管理的 Web 启用的工具。使用 PDM 的 PIX 远程管理在第 13 章中讨论
46	使用 PDM 创建一个站点对站点的 VPN	PIX 设备管理器 (PDM) 是一个用于 PIX 防火墙远程管理的 Web 启用的工具。使用 PDM 的 PIX 远程管理在第 13 章中讨论
47	使用 PDM 创建一个远程访问 VPN	PIX 设备管理器 (PDM) 是一个用于 PIX 防火墙远程管理的 Web 启用的工具。使用 PDM 的 PIX 远程管理在第 13 章中讨论
48	配置访问和转换规则	PIX MC 用于管理企业网络上的多个 PIX 防火墙。安装、配置和使用 PIX MC 在第 14 章中讲述
49	报告、工具和管理	PIX MC 用于管理企业网络上的多个 PIX 防火墙。安装、配置和使用 PIX MC 在第 14 章中讲述
50	介绍自动更新服务器 (AUS)	自动更新服务器 (AUS) 是 PIX MC 的一个部件,可以用于更新 PIX 防火墙。AUS 在第 14 章中讲述
51	PIX 防火墙和 AUS 通信设置	自动更新服务器 (AUS) 是 PIX MC 的一个部件,可以用于更新 PIX 防火墙。AUS 在第 14 章中讲述
52	设备、映像和分配	使用 PIX MC 和 AUS 在第 14 章中讨论
53	报告和管理	使用 PIX MC 和 AUS 在第 14 章中讨论
54	FWSM 概述	PIX FWSM 是向 Catalyst 6000 系列交换机提供 PIX 防火墙功能的关键部件。该部件在第 19 章中讲述
55	使用 PDM 和 FWSM	PIX FWSM 是向 Catalyst 6000 系列交换机提供 PIX 防火墙功能的关键部件。使用 PDM 管理该部件在第 13 章和第 19 章中讲述

Cisco 认证过程概述

网络安全市场当前的状况是对合格工程师的需求大大供不应求。因为这个原因,许多路由/网络方面的工程师正考虑转到网络安全方面。记住网络安全只是简单地将安全应用到网络中。这听起来像是一个显而易见的概念,但如果你要致力于安全认证的话,理解这一点是非

常重要的。在能够应用安全概念之前你必须非常熟悉网络。尽管开始 Cisco 安全认证过程不是非要先获得一个 Cisco 证书，但至少获得 CCNA 证书会非常有帮助。完成 CCNA 认证所需要的技巧给了你坚实的基础，你能够让它扩展到网络安全领域。

安全认证被称为 CCSP 认证，包括下列考试。

- CSPF——Cisco 高级安全 PIX 防火墙——642-521。
- SECUR——安全 Cisco IOS 网络（原来是 MCNS）——642-501。
- CSVPN——Cisco 安全虚拟专网——642-511。
- CSIDS——Cisco 安全入侵监测系统——642-531。
- CSI——Cisco SAFE 实现——642-541。

参加 CSPFA 认证考试

就像参加任何其他 Cisco 认证考试一样，在参加考试前最好做好充分的准备。没有办法知道在考试时会出什么样的题目，因此准备的最好方法是较好地掌握考试所涉及的全部知识点。要为考试做好计划，在参加考试前确保好好休息，为考试准备好精力。

跟踪 CCSP 状况

能够在 https://www.certmanager.net/~cisco_s/login.html 上通过查阅认证跟踪系统（the Certification Tracking System）来跟踪你的认证程序。在第一次登录该站点时你必须创建一个账户。

如何准备考试

准备任何认证考试的最好方法是组合使用准备资料、实验室和练习题。本书融入了一些实际问题和实验室的实践，能够更好地帮助你做准备。如果可能的话，你应当有一些亲自参与 Cisco PIX 防火墙实践的时间。没有什么能够代替实践，当真正地看到 PIX 在运转时，你就能够更容易理解这些命令和概念。如果你没有权力使用一个 PIX，那么就可以使用价格适当的大量模拟报文。最后，但不是最不重要的，Cisco 网站提供了关于 PIX 和与它交互产品的大量信息。没有哪个单一的资料能够满足为 CSPFA 考试准备的需要，除非你已经有大量使用 Cisco 产品的经验和组网或者网络安全方面的经历。最起码，你应该使用本书和 www.cisco.com/public/support/tac/home.shtml 为考试做准备。

评估你的考试准备情况

在完成了许多认证考试之后，我认为除非你解决了大约 30% 的问题，否则就不能真正知道是否为考试做了充分的准备。从这一点上讲，如果你没有准备好，那么就太晚了。首先，要确保为正确的考试做准备。认证考试 CSPFA 3.0 基本上是个新考试。确定你准备情况的最好方法是利用“我已经知道了吗？”测试题、每章后面的问答题，以及案例研究和场景。最好是兢兢业业读完全书，除非你不做任何探讨或者查找任何答案就能够完成每个问题。