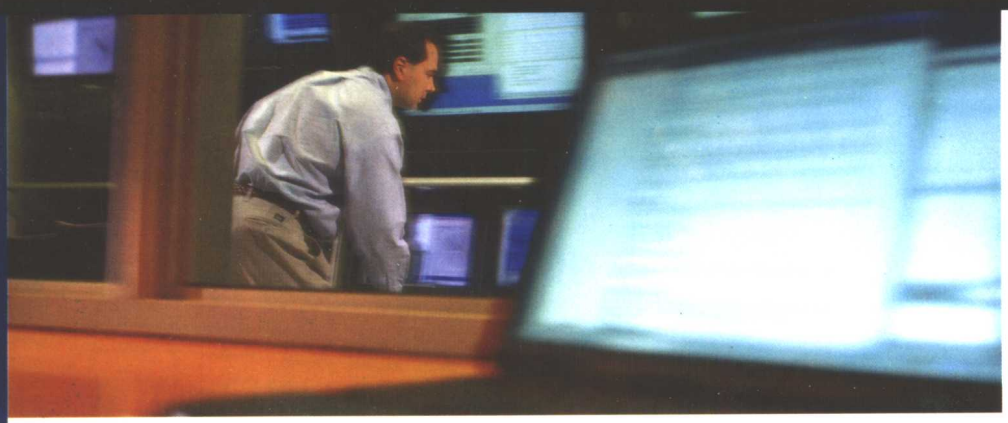
Cisco 职业认证培训系列
CISCO CAREER CERTIFICATIONS

ciscopress.com



CCSP Cisco 安全 PIX 防火墙认证考试指南

CCSP™ Self-Study

CCSP Cisco Secure PIX® Firewall Advanced

Exam Certification Guide

Official self-study test preparation guide for the Cisco 9E0-111 and 642-521 CSPFA exams

内附光盘

[美] Greg Bastien
Christian Abera Degu 著
卢泽新 孙志刚 白建军 靳济方 译

人民邮电出版社
POSTS & TELECOM PRESS

内容提要

本书是为那些对安全认证感兴趣的安全专业人员和网络专业人员设计的，目的是帮助他们通过 9E0-111 或者 642-521 Cisco PIX 防火墙高级（CSPFA）认证考试。全书共分 15 章，分别介绍了网络安全、防火墙技术和 Cisco PIX 防火墙、系统维护、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、Cisco PIX 防火墙故障切换、虚拟专用网、PIX 设备管理员、用 Cisco PIX 防火墙进行内容过滤、AAA 和 Cisco PIX 防火墙概述、Cisco PIX 防火墙上的 AAA 配置、攻击防护和多媒体支持等。

本书适合参加 CCSP 认证考试中关于 PIX 防火墙考试的应试者阅读。

关于作者

Greg Bastien：CCNP、CCSP、CISSP，现在是 True North Solutions 公司的高级网络安全工程师，美国国家部门的顾问。他是 Strayer 大学的兼职教授，教授网络和网络安全教程。当他在美国军队作为一个直升飞机飞行教官期间，在 Embry-Riddle 航空大学完成了他的本科和研究生学位。他和他的妻子、两个儿子生活在 Maryland 州的 Monrovia。

Christian Degu：CCNP、CCDP、CCSP，现在是联邦能源管理委员会的一名顾问工程师。他是 Strayer 大学的兼职教授，教授计算机信息系统课程。他有一个计算机信息系统的硕士学位，居住在 Virginia 州的 Alexandria。

关于技术审稿人

Will Aranha 现在是 Symantec 公司的首席安全工程师。他的主要工作是作为技术产品的管理员，包括决定新产品支持、基准，以及为安全技术人员提供技术培训。Aranha 在许多信息安全产品和实践方面非常精通。随着美国和国际上许多防火墙/VPN 和 IDS 的配备，他作为一个所有管理服务所支持产品的问题专家，为一个 24/7 安全操作中心（Security Operations Center）提供第 3 方的技术支持。Aranha 也为 Riptech 公司（已被 Symantec 公司所兼并）的成长和发展作出了贡献。

Mesfin Goshu，CCIE No.8350，是 Metrocall Wrieless 公司的系统工程师，该公司是美国第二大无线公司。他负责设计、维护、故障诊断和 Metrocall 公司的主干网络安全。他在 Metrocall 公司几乎有 6 年了，在 OSPF、BGP、MPLS 和网络安全方面有着大量的阅历。他有一个计算机和信息科学与民用工程的理学学士学位，现在正为一个远程通信的理学硕士学位而学习。作为一个高级的网络工程师，他以一个承包人的身份而致力于 INS 和 Pentagon 的工作。他在网络领域工作已经超过 9 年了。

Jonathan Limbo，CCIE 安全 No.10508。现在作为一个安全和 VPN 支持的工程师，负责 PIX 以及其他安全和 VPN 产品的升级工作。Jonathan 在 IT 行业已经工作了 5 年了，其中的大部分时间作为一个网络工程师。

Gilles Piché 是一位安全顾问，他在加拿大从事网络安全领域的工作已经有 6 年多了。在此之前，他与加拿大政府签约在网络工程技术性能方面工作。Gilles 也是一个 Cisco 安全认证的讲师，最近两年间在 Global Knowledge Network（加拿大）公司讲授 Cisco 安全课程。

献　辞

献给 Ingrid、Joshua 和 Lukas，在我泡在办公室里时，谢谢你们能够容忍我。——Greg

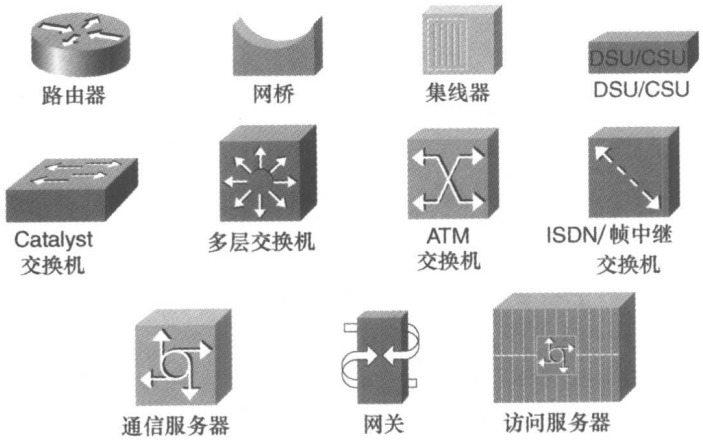
献给我的父亲 Aberra Degu 和我的母亲 Tifsehit Hailegiorgise，谢谢你们对我的鼓励和爱。献给我的弟弟 Petros 和妹妹 Hiwote 和 Lula，我爱你们。——Christian

致　谢

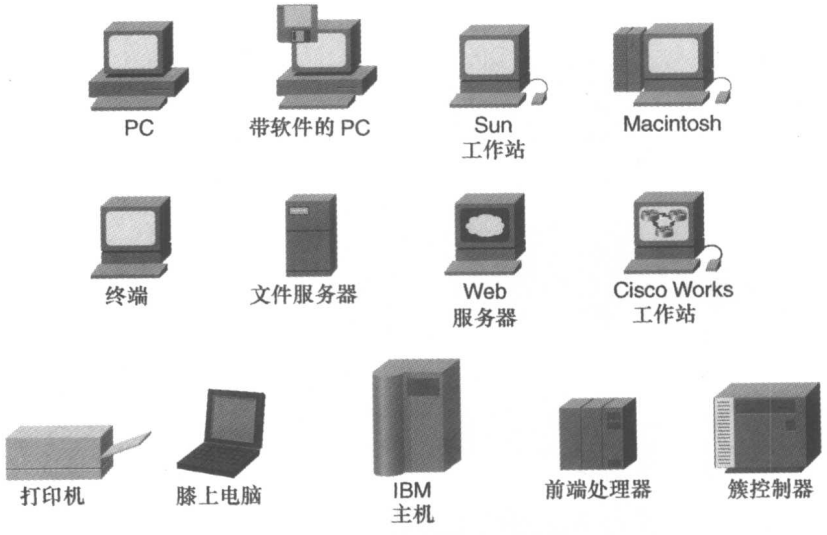
写这本书是一个困难而耗时的工作，但又是一个非常有益的工作。许多人以某种形式或者某种方式为本书的出版作出了贡献。我们特别要感谢Cisco Press团队，包括Michelle Grandin和Christopher Cleveland，感谢他们在整个写书过程中的指导和鼓励。我们也要感谢技术审稿人，感谢他们能够忍受我们潦草的底稿，并在整个过程中帮助我们保持在正确的方向上。

本书使用的图标

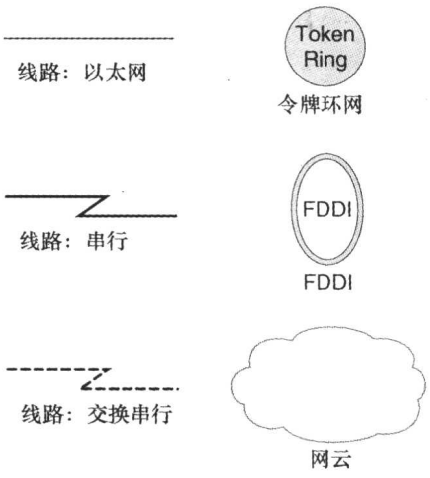
贯穿本书，你可以看到用于网络设备的下列图标：



下面的图标用于外围设备和其他设备：



下面的图标用于网络和网络连接：



前　言

本书的主要目的是在你为获得 CCSP 或者 PIX 认证而努力时，帮助你通过 9E0-111 或者 642-521 Cisco PIX 防火墙高级（CSPFA）认证考试。

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的概念是非常重要的。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 15 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）或者配置实践。附录 B 包括一个组合了许多不同知识点的附加的“高级”案例研究。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。

这些章节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，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”**——第 3 章更详细地

讨论了 Cisco PIX 防火墙的设计。本章列出了不同的 PIX 型号和它们的应用目标，并讨论了每种型号可用的各种特性以及每种型号是如何实现的。

- **第 4 章，“系统维护”**——第 4 章讨论了 Cisco PIX 防火墙 OS 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** 防火墙转换和连接”——本章涉及不同的转换协议以及 PIX 防火墙是如何处理它们的。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”**——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，“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 10 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。第 10 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 11 章，“PIX 设备管理员”**——能够使用多种工具管理 Cisco PIX 防火墙。第 11 章讨论了 PIX 设备管理员，它是一个能够用于管理 PIX 的基于 Web 的图形用户接口（GUI）。
- **第 12 章，“用 Cisco PIX 防火墙进行内容过滤”**——将攻击代码置入到一个 Web 页的内容之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。本章也涉及过滤通过防火墙的潜在恶意流量的不同 PIX 配置。
- **第 13 章，“AAA 和 Cisco 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。本章讨论配置认证、授权和统计（AAA）服务的 PIX 防火墙的不同型号。本章也介绍 Cisco 安全访问控制服务器（CSACS），它是 Cisco 的 AAA 服务器组件。
- **第 14 章，“Cisco PIX 防火墙上的 AAA 配置”**——本章讨论为与 AAA 服务器通信而在 PIX 防火墙上的特殊配置，包括 CSACS。涉及 PIX 防火墙上 AAA 的实现、功能性和故障查找。
- **第 15 章，“攻击防护和多媒体支持”**——能够对网络和它的周边设备发动许多不同类型的攻击。本章讨论了大部常见的攻击，以及怎样配置 PIX 防火墙来抵制这些攻击。

本书中每章都有相同的格式，并且融入了下面的特征，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。

- **“我已经知道这些了吗？”测试**——每章的开始都有一个测试，帮助你评估当前所掌握的本章的知识有多少。这个测试主要涉及所强调的特定领域，从而帮助你当开始本章的学习时确定把重点放在什么地方。
- **基础知识点**——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。
- **基础知识小结**——在每章的结尾，都要将本章的基础知识点总结成重点集锦。在大部分情况下，基础知识点总结在表格中。但在另一些情况下，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知识部分是帮助你为考试做准备的。虽然基础知识点和基础知识小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。
- **Q&A**——每章都以一系列测试你对本章材料理解程度的复习题结束。这些习题是确保你不但理解本章中的材料，而且是锻练你回忆事实的好方法。
- **案例研究/场景**——这些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构件是如何影响其他构件的。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。这里也有一部分可行或者不可行的配置，你要正确地确定它们是否可行，并且为什么可行或者不可行。因为认证考试要问关于 Cisco PIX 防火墙的特殊问题，因此非常熟悉不同的命令和 PIX 配置的构件非常重要。
- **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。使用我们的可定制的考试引擎，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，或者是一些随机的问题。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。

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。这也就是说要*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“基础知识点”并且将它们贯穿于本书的始末。表 1-1 描述了每个基础知识点。

表 1-1　CSPFA 基础知识点

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 防火墙概述	第 2 章讨论了 PIX 防火墙的设计，以及与其他防火墙产品相比它的优势
3	PIX 防火墙型号	当前，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
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

续表

参考号	考点	描述
6	配置 PIX 防火墙	许多不同的命令用于配置 PIX 防火墙。这些命令在第 6 章到第 15 章讨论
7	检验 PIX 防火墙状态	验证 PIX 防火墙配置能够帮助你查找连通性的问题
8	时间设置和 NTP 支持	确保防火墙时间与网络时间同步是重要的。第 6 章涉及在 PIX 防火墙上配置时间的命令
9	ASA 安全等级	自适应安全算法是 PIX 防火墙的一个关键构件。在第 2、3、5 和第 6 章更详细地讨论了这个问题
10	基本 PIX 防火墙配置	PIX 防火墙的基本配置在第 6 章中讨论
11	系统日志配置	第 8 章涉及 PIX 防火墙的日志特性
12	路由配置	因为防火墙操作在 OSI 模型的多个层上，它能够路由流量，也能够过滤流量。PIX 防火墙的路由命令在第 6 章讨论
13	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 章和第 6 章涉及这些配置
14	传输协议	传输层协议和 PIX 防火墙如何处理它们在第 5 章讨论
15	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络段的安全。这在第 5 章和第 6 章讨论
16	端口地址转换	端口地址转换是 PIX 防火墙用于将多个内部源 NAT 到一个单独的外部地址的一个方法。第 5 章和第 6 章涉及这个配置
17	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 5 章讨论
18	ACL	访问控制列表用于允许或者拒绝通过 PIX 防火墙的不同网络段间的流量。配置 ACL 在第 7 章讨论
19	使用 ACL	配置 ACL 在第 7 章讨论
20	URL 过滤	可以配置 PIX 防火墙与其他产品一起工作执行 URL 内容过滤。做到这一点以确保用户依照公司的政策使用公司的资产。配置 PIX 内容过滤在第 12 章讨论
21	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 章讨论
22	开始使用组对象	对象分组在第 7 章讨论
23	配置组对象	对象分组在第 7 章讨论
24	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 章讨论
25	高级协议	许多高级协议需要防火墙的特殊处理。一些协议需要多个输入和输出的连接。PIX 防火墙处理的高级协议在第 7 章讨论
26	多媒体支持	多媒体协议被看成高级协议。PIX 防火墙处理的高级协议在第 7 章讨论
27	攻击防护	能够配置 PIX 防火墙辨别一个攻击并对它作出反应。这在第 15 章讨论
28	入侵检测	能够配置 PIX 防火墙作为一个入侵检测系统和一个防火墙来运行。也能够与外部 IDS 一起工作。这些问题在第 15 章讨论
29	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 13 和 14 章讨论
30	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 13 章讨论

续表

参考号	考　点	描　述
31	认证配置	配置 CSACS 在第 13 章和 14 章讨论
32	可下载的 ACL	配置 CSACS 在第 13 章和 14 章讨论
33	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。能够配置两个防火墙作为一个高可用性的方案。这个配置在第 9 章讨论
34	故障切换配置	PIX 故障切换配置在第 9 章讨论
35	基于 LAN 的故障切换配置	PIX 故障切换配置在第 9 章讨论
36	PIX 防火墙激活一个安全 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 10 章讨论
37	IPSec 配置任务	配置虚拟专用网在第 10 章讨论
38	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 10 章讨论
39	配置 IKE 参数	IKE 是用于确保加密连接不容易被破解的一个密钥交换的方法。配置虚拟专用网在第 10 章讨论
40	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 10 章讨论
41	测试和验证 VPN 配置	虚拟专用网的配置和故障查找在第 10 章讨论
42	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 10 章讨论
43	衡量 PIX 防火墙 VPN	配置虚拟专用网在第 10 章讨论
44	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 10 章讨论
45	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 章讨论
46	命令级授权	PIX 防火墙的远程管理在第 4 章讨论
47	PDM 概述	PIX 设备管理员（PDM）是一个用于 PIX 防火墙远程管理的 web 激活的工具。使用 PDM 的 PIX 远程管理在第 11 章讨论
48	PDM 操作要求	PIX 设备管理员（PDM）是一个用于 PIX 防火墙远程管理的 web 激活的工具。使用 PDM 的 PIX 远程管理在第 11 章讨论
49	PDM 准备	PIX 设备管理员（PDM）是一个用于 PIX 防火墙远程管理的 web 激活的工具。使用 PDM 的 PIX 远程管理在第 11 章讨论
50	使用 PDM 配置 PIX 防火墙	PIX 设备管理员（PDM）是一个用于 PIX 防火墙远程管理的 web 激活的工具。使用 PDM 的 PIX 远程管理在第 11 章讨论
51	使用 PDM 创建一个站点对站点的 VPN	PIX 设备管理员（PDM）是一个用于 PIX 防火墙远程管理的 web 激活的工具。使用 PDM 的 PIX 远程管理在第 11 章讨论
52	使用 PDM 创建一个远程访问 VPN	PIX 设备管理员（PDM）是一个用于 PIX 防火墙远程管理的 web 激活的工具。使用 PDM 的 PIX 远程管理在第 11 章讨论

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要求大大供不应求。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。所有 CCSP 报考者必须首先通过 Cisco 认证网络工程师（CCNA）考试。完成 CCNA 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。

表 1-2 包含了一列 CCSP 认证系列的考试。因为所有的考试信息是由 Cisco Systems 管理的，因此易于发生变化。考生应该经常到 Cisco Systems 的站点，www.cisco.com/go/training，查找课程和考试的更新信息。

表 1-2　　CCSP 认证考试

考试编号	考试名	即将到来的考试变更说明
640-100	MCNS 3.0，管理 Cisco 网络安全	在 2003 年夏季，开始执行一个新的考试，SECUR 642-501。这个新的考试将最终代替 640-100 考试。如果重新认证的考生通过这个考试，他们会被考虑换发 CCNA 或者 CCDA 等级的证书
9E0-111	CSPFA 3.0，Cisco 安全 PIX 防火墙高级考试	2003 年夏季前后，将采用一个新的 PIX 考试来认证考生：642-521。注意这个重编的数字，通过这个考试会被考虑换发 CCNA 或者 CCDA 等级的证书。9E0-111 考试和 642-521 考试之间没有重大的差别
9E0-100	CSIDS 3.0，Cisco 安全入侵检测系统	在本书出版的时候还没有关于这个考试的预计变化情况。一定要到 Cisco Systems 的站点上查阅关于考试编号和内容的变化信息
9E0-121	CSVPN 3.0，Cisco 安全虚拟专用网	2003 年夏季前后，将采用一个新的 VPN 考试来认证考生：642-511。注意这个重编的数字，通过这个考试会被考虑换发 CCNA 或者 CCDA 等级的证书。9E0-121 考试和 642-511 考试之间没有重大的差别
9E0-131	CSI 1.0，Cisco SAFE 实现	在本书出版的时候还没有关于这个考试的预计变化情况。一定要到 Cisco Systems 的站点上查阅关于考试编号和内容的变化信息

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考点知识。为考试做好计划，在参加考试前确保好好休息并对焦点问题作好了准备。

找到 Cisco 培训和认证最新资料的最好地方是 www.cisco.com/go/traning.。

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。你必须创建一个帐户，使用你成绩报告单上的信息，在第一时间登录这个站点。考试结果在保持 10 天后会被更新。

如何为这个考试做准备

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.com 提供了关于 PIX 和与它交互的所有产品大量信息。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 产品的经验和网络或者网络安全的背景。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，我发现除非你解决了大约 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，始终要确保为正确的考试做准备。本书帮助你为下面两种 CSPFA 考试评估准备情况：9E0-111 和 642-521。确定你准备情况的最好方法是通过“我已经知道这些了吗？”测验题、每章后面的 Q&A，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。

现实世界的 Cisco 安全专家

Cisco 是 Internet 上最被公认的名字之一。没有看到一些 Cisco 认证你就不能进入一个数据中心或者服务器机房。Cisco 认证的安全专家能够将相当多的知识带到讲桌上来，是归因于他们对网络和网络安全之间关系的深刻理解。这也是 Cisco 认证为什么会带来如此的影响力。Cisco 认证向潜在的雇主和合同持有人证明了一个明确的专家地位和完成一个目标的专用要求。记住这一点：如果这些认证容易得到的话，那么每个人都会有。

PIX 和 Cisco IOS 软件命令

防火墙或者路由器不是可以乱动的平常东西。在适当地配置好它们以后，你就会让它们单独工作，直到出问题或者需要做一些其他的配置更改。这也就是为什么问题标志（？）可能是最大量使用的 Cisco IOS 命令的原因。除非你经常地使用这个设备，否则很难记住配置设备和查找故障所需的众多命令。大部分的工程师只记住了完成正确方向所需的足够命令，然后使用（？）来调用正确的语法。这就是现实世界的生活。但是，（？）在测试环境下是不可用的。考试中的许多问题需要你选择最好的命令去执行某种功能。因此熟悉不同的命令以及它们各自的功能极其重要。

本书中使用的约定

本书使用 Cisco Systems 公司的下面语法约定：

- ***黑体***表示用户逐字键入的一个命令或者关键字
- *斜体*表示用户提供值的一个命令参数或者选项。
- 垂直线/管状符号（|）分隔备选项、相互排斥的命令选项。也就是说，用户只能键入一个并且只能是一个被管状符号分开的选项。
- 方括号（[]）表示命令的一个任选元素。
- 大括号（{}）表示命令必须的选项。用户必须键入这个选项。
- 方括号内的大括号（[{}]）表示如果用户执行这个命令可选元素的一个必须选择。

道路规则

我们总是能够发现在一本技术出版物中，当示例中使用不同的地址时总会引起混乱。为此，我们在本书中分配网络段时使用如图 I-1 所示的地址空间。注意，我们选择的地址空间是每个 RFC 1918 都保留的空间。我们理解这些地址不能被 Internet 路由，并且通常不用于外部接口。即使是在 Internet 中有上百万的 IP 地址可选择以使用，因为它们的拥有者不想将这些地址出版在本书中，所以我们能够选择的地址是非常少的。

能够帮助你理解配置和管理 Cisco PIX 防火墙所需的众多命令的例子和语法正是我们的希望。

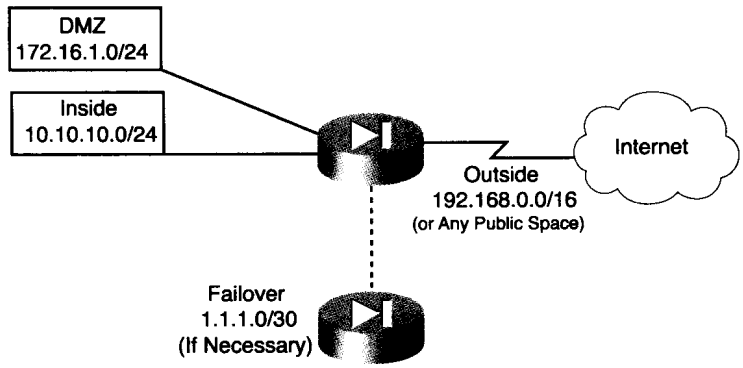


图 I-1 地址示例

目　录