CCSA NG: Check Point Certified Security Administrator Study Guide

CCSA NG: Check Point

认证安全管理员全息教程

考试号：156-210

〔美〕 Justin Menga 著

马树奇 金 燕 等译

全球最优秀的出版社之一
各种SYBEX学习指南书籍
印数已经超过500万册

SYBEX

美迪亚

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

CCSA NG: Check Point Certified Security Administrator Study Guide

CCSA NG：Check Point 认证安全管理员全息教程

〔美〕 Justin Menga 著

马树奇 金 燕 等译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 提 要

在Check Point公司针对其产品推出的多项认证中，安全管理员认证是一项基础认证，用于证明申请者配置和管理FireWall-1基本系统的能力。本书针对这一认证的考试目标，围绕VPN-1/FireWall-1产品的体系结构、安全策略、身份验证、网络地址翻译、备份与恢复等关键点进行了详细介绍。此外，本书秉承边学边练、学以致用的思想，提供了很多练习机会，同时在每一章的结尾给出了相关内容的复习题及答案。

相信本书可以为期望获得Check Point认证安全管理员资格的应试者和Check Point防火墙的使用者提供有益帮助。

版权贸易合同登记号：01-2003-1093

图书在版编目（CIP）数据

CCSA NG：Check Point认证安全管理员全息教程/（美）门格（Menga, J.）著；马树奇等译.—北京：电子工业出版社，2003.7

书名原文：CCSA NG: Check Point Certified Security Administrator Study Guide

ISBN 7-5053-8769-3

Ⅰ. C… Ⅱ. ①门… ②马… Ⅲ. 计算机网络－安全技术－工程技术人员－资格考核－教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2003）第041693号

责任编辑：李 莹

印 刷：北京天竺颖华印刷厂

出版发行：电子工业出版社 http://www.phei.com.cn

北京市海淀区万寿路173信箱 邮编：100036

北京市海淀区翠微东里甲2号 邮编：100036

经 销：各地新华书店

开 本：787×1092 1/16 印张：29.25 字数：740千字

版 次：2003年7月第1版 2003年7月第1次印刷

定 价：48.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换，若书店售缺，请与本社发行部联系。联系电话：（010）68279077

致读者

Check Point公司的认证在IT安全领域厂商认证中名符其实地占据着主导地位。随着新版Check Point NG考试的推出，大量有抱负的安全领域专业技术人员开始寻找内容准确、细致的学习材料，用来帮助他们为新推出的CCSA和CCSE考试做准备。

Sybex公司能够为大家提供在竞争激烈的IT安全领域取得成功所需的知识和技能，对此我们深感荣幸。Sybex公司将一如继往地以向广大应试者提供现实世界中的大量新技术并解释其工作过程为己任，而并不只是简单地告诉读者相关试题的答案是什么。Sybex公司的立足点在于向IT专业人士提供所需的技能，以后也将继续遵循这个原则。多年来，我们已经根据广大读者的反馈意见、相关教师的建议以及行业领导者的说明，对推出的全息教程系列丛书进行了大量的改进。

Check Point公司的认证考试确实很富于挑战性。Sybex公司的作者、编辑以及技术监督组成的开发队伍正在努力工作，以保证我们的全息教程系列丛书内容广泛、深入并且遵循科学的教育方法。我们相信，本书以及可供读者选购的光碟中包含的最先进的软件学习工具将能够满足并且超过认证市场的相关标准，能够帮助广大将要参加Check Point认证考试的读者达到自己的目标。

祝大家在取得Check Point认证的道路上一帆风顺！

Neil Edde
认证副总编
Sybex公司

简　介

欢迎参加激动人心的Check Point认证！大家选择了这本书肯定是因为希望获得更好的工作机会，获得事业上更大的成功。这是个明智的选择，因为对于尚未找到工作的人而言，Check Point认证能够帮助你们获得自己的第一份网络或安全方面的工作；对于已经在此领域工作的专业人士，Check Point认证可以给其拥有者带来更丰厚的报酬或者晋升机会。

Check Point认证也有助于大家更好地理解包括Check Point公司产品在内的网络安全技术如何工作。例如，目前有300多种产品通过IP语音（Voice over IP，VoIP）和轻型目录访问协议（Lightweight Directory Access Protocol，LDAP）之类的协议集成了VPN-1/FireWall-1，其中还有其他一些技术，如网络地址翻译（Network Address Translation，NAT）以及分组内容过滤。Check Point公司还为其开放安全平台（Open Platform for Security，OPSEC）制订了一系列标准，以便于用户在Check Point产品中使用第三方厂商开发的产品。该机构的网址是www.opsec.com。

Check Point公司自从1995年以来就已经在全球的防火墙及VPN产品市场上居于领先地位，因此获取Check Point认证当然会给大家带来益处。根据Check Point公司网站的报告，该公司的产品解决方案“已经由世界上149个国家的2500家经过认证的合作伙伴销售、集成和服务，组成了一个庞大的网络。”申请者获得了Check Point认证后就可以成为一名Check Point认证的专业人员（Check Point Certified Professional，CCP），进而获得使用认证专业人员密码保护网站（Certified Professional password-protected website）的资格。在这里，经过认证的专业人员可以找到普通人无法获得的工具、特殊功能、誊本以及其他有关信息。CCP还可以访问SecureKnowledge知识库，得到关于产品更新的通知，有资格使用相关的徽标和凭证，以及在Check Point公司的年会及其他活动中受到邀请。如果读者想了解关于CCP认证程序的更多信息，请访问网站www.checkpoint.com/services/education/certification/index.html。

在获取Check Point认证的过程中，大家会更全面地理解网络安全的各个层面。这些知识将会对所有从事网络安全的人有益，这也是目前Check Point认证如此流行的原因。Check Point公司是目前世界上防火墙和VPN（虚拟专用网络）领域居于领先地位并且受人尊敬的厂商。为了保证有关机构能够正确地评价其Check Point管理员及工程师的技术水平，Check Point公司提供了多种层次的认证，能够以准确的量化方式衡量他们在网络安全方面的知识，以及评价系统管理员使用Check Point产品实施网络安全保护的能力。

如何使用本书

如果读者希望为通过Check Point认证安全管理员（Check Point Certified Security Administrator，CCSA）考试打下坚实的基础，那么本书定能如你所愿。我们在编写本书时，花了大量的时间和精力，使之能够最好地帮助读者通过VPN-1/FireWall-1 Management I NG （156-210）考试。

本书载有大量宝贵的信息，如果读者能够对本书的构成有所理解，那么就更容易在学习过程中获得最充分的收益。

为了获得最理想的学习效果，建议大家在本书的学习过程中遵循下列学习方法：

1. 阅读完这份简介之后，立即进行评估考试（答案附在评估考试的后面）。对于其中的任何问题，如果读者不知道其答案，没有关系，这就是学习本书的原因！对于自己答错的题目，应认真阅读后面的解释，并且注意相关的知识在哪些章节介绍。这些信息可以帮助读者安排自己的学习过程。
2. 认真地学习每一章，一定要完全理解书中的信息以及每一章开始部分列出的考试目标。对于自己在评估考试中答错了有关问题的章节更要额外给予关注。
3. 尽可能独立地完成每一章后面给出的练习。如果自己确实没有Check Point VPN-1/FireWall-1设备和相关软件，那么一定要认真学习书中提供的示例。
4. 认真回答每一章给出的所有复习题（答案列在每一章的最后）。注意容易引起混淆的问题，并且反复学习书中有关的内容。千万不要忽略这些问题！一定要保证自己完全理解了每个答案。
5. 在本书的选购光碟中提供了模拟考试，读者可以在这里试一试自己的身手。注意，模拟考试仅在选购光碟中提供。这些考试能够让读者更全面地感受到自己在真正的VPN-1/FireWall-1 Management I NG考试中将会遇到的情况。
6. 读者也可以使用选购光碟中提供的电子助记卡程序进行测验。这张光碟提供了最新的电子助记卡程序，可以帮助读者更全面地为参加VPN-1/FireWall-1 Management I NG考试做好准备。这些都是非常出色的学习工具！

提示： 电子助记卡程序可以在Windows计算机、便携式PC或者掌上型设备中使用。

7. 一定要阅读各章后面列出的关键术语和考试要点。这些辅助内容能够帮助读者在每一章内容学习完毕之后，对于其中的要点有清晰的认识；这些内容还可以供考生在进入考试中心之前作为复习的要点。

为了完成本书中指出的所有学习内容，读者必须定期学习，并且要自律。应该努力规定每天在相同的时间段，选择一个舒适、安静的地方进行学习。只要大家努力，就一定会对自己学习这些材料获得的效果感到惊讶和高兴。

只要大家遵循上述步骤，认真学习和完成复习题、选购光碟上的考试题以及使用电子助记卡，就完全能够通过VPN-1/FireWall-1 Management I NG考试。

本书包含的内容

本书的内容涵盖了应试者通过VPN-1/FireWall-1 Management I NG考试所需的全部知识。

- 第1章介绍Check Point公司的安全虚拟网络（Secure Virtual Network），这是一个提供了全面实现端对端（end-to-end）网络安全解决方案的框架。这一章还要对Check Point公司的VPN-1/Firewall-1产品进行比较概括的介绍。
- 第2章介绍的是防火墙应用的不同类型的体系结构，并且将较细致地讨论VPN-1/FireWall-1的体系结构。

- 第3章介绍VPN-1/FireWall-1安全策略的基本情况，涉及构成其安全策略数据库的各个组件，以及安全对象、安全属性和安全规则等概念。我们期望在这一章将要结束的时候，读者能够使用安全规则配置一个复杂的安全策略，并且在VPN-1/FireWall-1执行模块上安装相应的策略。
- 第4章讨论的是高级安全策略主题，包括如何优化安全策略的性能以及如何更有效地管理安全规则库。读者还将学习许多有用的CLI实用程序，用以管理和监视VPN-1/FireWall-1。
- 第5章介绍的是如何使用SmartView Tracker应用程序，以保证自己正确地使用VPN-1/FireWall-1自带的安全日志记录功能、检测安全方面存在的威胁，以及中断存在安全隐患的相应连接。
- 第6章讨论的是VPN-1/FireWall-1的身份验证以及VPN-1/FireWall-1如何支持众多流行的身份验证方案。读者在这里还将学习到如何配置用户数据库，以有效地存储所有用户和组对象，因为这些内容在定义身份验证规则时都十分重要。
- 第7章将深入地分析VPN-1/FireWall-1支持的每一种身份验证类型、如何实现各种身份验证类型以及何时实施每一种身份验证。
- 第8章介绍网络地址翻译（Network Address Translation，NAT）的概念、为什么NAT会成为目前因特网连接中不可缺少的组件，并且讨论NAT的各种不同类型以及它们的优点和缺点。
- 第9章介绍如何在VPN-1/FireWall-1上配置网络地址翻译。读者将学习如何配置自动NAT和手动NAT。在这里我们还将深入探讨各种不同类型的NAT之间的区别以及相应的注意事项，以便于大家能够知道何时应该实施何种类型的NAT比较适合。
- 第10章介绍的是进行VPN-1/FireWall-1备份和恢复时所需的信息，以保证VPN-1/FireWall-1系统具有持久的可用性和可靠性。读者还将学习如何卸载VPN-1/FireWall-1系统，这也是恢复过程中可能需要的操作。最后，学习关于SmartView Status SMART客户程序的知识。这种客户程序用来对VPN-1/FireWall-1系统及产品进行实时监视，以保证系统中发生任何潜在问题时用户都能够得到及时的通知。
- 在本书的词汇表中收集了Check Point公司及其他相关领域的安全词汇，使用非常方便。读者可以把它作为一个理解书中有关术语的出色工具。

每一章开始的部分都会列出该章内容覆盖的VPN-1/FireWall-1 Management I NG考试目标。注意一定要在阅读有关章节的内容之前先查看这里列出的考试目标。此外，每一章结束的部分都会列出相关的复习题。这些复习题是专门设计用来帮助读者复习书中有关信息的。为了真正了解自己掌握的技能，应该认真阅读每一道复习题，如果可能的话，还要完成有关章节中列出的动手练习。

说明： 在Check Point NG中有定期发布的软件更新。在过去几年中，Check Point公司发布了许多服务包，通过修补程序和增强代码来改善其当前的产品。Check Point公司还会通过NG发布功能包（Feature Pack，FP），其中不仅包含修补程序，而且还提供显著的特性及增强代码。在编写本书的时候，FireWall-1使用的最新版本是Check Point NG Feature Pack 3。由于该版本进行了广泛的性能增强，因此读者应该将此版本作为自己进行系统部署的最低标准，同时它也是本书内容编写的基础。

选购光碟中的内容

我们正在努力工作，以便提供一些良好的工具，帮助读者获得认证。在读者学习并准备通过认证考试的时候，应该将下列工具全部安装到自己的工作站上并且正确地使用。

全新的Sybex考试准备软件

由Sybex公司的专家们开发的考试准备软件可以帮助应试者通过VPN-1/FireWall-1 Management I NG考试。在这个考试软件中，应试者可找到书中的全部复习题和评估考试题，另外还有两套在光碟中独有的模拟试卷。应试者可以对自己进行评估考试、按章节或者主题进行自我测验，也可以使用从全部试题中随机生成的试卷进行考试。

用于PC机、便携式PC及掌上设备的电子助记卡

为了参加认证考试，大家可以阅读本书、完成动手练习、完成每一章后面的复习题，以及参加书中和选购光碟中附带的模拟考试。我们提供的辅助手段还不止这些。读者还可以使用选购光碟中提供的电子助记卡程序进行自我测验。如果读者能够解答这些较难的题目并且理解有关的答案，那么就已经为VPN-1/FireWall-1 Management I NG考试做好了准备。

电子助记卡中包含150道专门针对一些难点而设的题目，以保证考生确实为考试做好了准备。有了复习题、模拟考试和电子助记卡，各位所达到的水平定会超出认证考试的要求。

PDF格式的CCSA全息教程

Sybex公司在选购光碟上提供了PDF格式的CCSA Study Guide（CCSA全息教程），以便于读者在PC机或者便携式电脑上阅读。对于旅途中的读者、不想带书的读者或者喜欢在计算机上阅读的人们来说，这是个很好的帮手（注：选购光碟中提供的是英文原版）。在选购光碟中还提供了Acrobat Reader 5程序。

Check Point公司简介

Check Point Software Technologies（Check Point软件技术公司）1993年由Gil Shwed、Marius Nacht和Shlomo Kramer创办，并且迅速成长为全球因特网、网络安全、VPN和防火墙市场的业界领先者。Check Point公司一开始的时候只是一家小型的软件公司，现在已经成为信息安全领域的国际领先企业，拥有1000多名员工，2001年的收入超过了5亿美元。该公司的国际总部在以色列的Ramat-Gan市，其在美国的运营基地位于加利福尼亚州的Redwood市。

Check Point公司的产品如Check Point VPN-1/FireWall-1、Provider-1和FloodGate-1都以安全虚拟网络（Secure Virtual Network，SVN）作为其基本的体系结构。该公司正在不断使其安全领域的产品推陈出新，为因特网和网络安全领域提供最好的解决方案。他们的OPSEC伙伴联盟对Check Point产品的功能进行了扩展，使之能够与超过325家的各领域领先的企业产品集成并且实现互操作。

从1997年开始，Check Point公司每年都会赢得大奖。2000年10月，他们的产品被Network Computing杂志评选为“10年来最重要的产品”十强之一。

Check Point公司的VPN-1/FireWall-1获得了无数的认证，其中既包括美国，也包括许多其他国家，因为该公司的产品符合世界各国政府和商业团体制定的严格的安全标准。Check Point NG获得了下列认证：

- 信息技术安全鉴定的通用标准（Common Criteria for Information Technology Security Evaluation，CCITSE）：这是由美国国家安全总署/国家标准和技术研究所（U.S. National Security Agency/National Institute of Standards and Technologies）以及其他13个国家的相应机构共同制定的评估条件。信息技术安全评估基本条件（简称CCITSE或者“基本条件”）是多国机构在以前使用的可信任的计算机系统评估条件（Trusted Computer System Evaluation Criteria，TCSEC）基础上，经过努力而编写出的后继标准。关于CCITSE的情况读者可以通过网址www.radium.ncsc.mil/tpep/library/ccitse/查阅。
- 美国国家标准和技术研究所（NIST）管理的联邦信息处理标准（Federal Information Processing Standard，FIPS）140-1 level 2认证和加拿大政府制定的通信安全规定（Communications Security Establishment，CSE）制定了一系列关于信息系统安全的要求，以保护系统抵抗潜在的黑客及信息犯罪的威胁。关于FIPS的信息读者可以通过网址www.itl.nist.gov/fipspubs/index.htm查询。
- 英国通信电子安全组织（Communications Electronics Security Group，CESG）制定的IT安全鉴定标准（IT Security Evaluation Criteria，ITSEC E3）与Common Criteria EAL 4标准相当，相关的内容可以从下列网址查询：www.cesg.gov.uk/assurance/iacs/itsec/index.htm。

Check Point公司的VPN-1/FireWall-1安全认证

Check Point公司推出了许多针对其产品进行的认证。首先推出的是Check Point认证网络助理（Check Point Certified Network Associate，CCSA）、Check Point认证网络专家（Check Point Certified Network Expert，CCSE）和CCSE Plus，这些认证都建立在VPN-1/FireWall-1产品的基础上。获得这些认证后，申请人可以继续获取其他称号，如针对FloodGate-1产品的Check Point认证服务质量专家（Check Point Certified Quality of Service Expert，CCQE），以及针对Meta IP产品的Check Point认证编址专家（Check Point Certified Addressing Expert，CCAE）等。最后，对于参与实现VPN-1/FireWall-1和Provider-1因特网安全解决方案的工程师，Check Point公司提供了高级Check Point认证的托管安全专家（Check Point Certified Managed Security Expert，CCMSE）认证。要想获得此项认证，申请者必须先通过CCSA、CCSE和Managing Multiple Sites with Provider-1（用Provider-1管理多个网站）考试。

Check Point认证安全管理员

Check Point认证安全管理员（Check Point Certified Security Administrator，CCSA）是一项基本认证，用来证明申请者配置和管理FireWall-1基本系统的能力。在获得此项认证之前，申请者必须掌握定义和配置安全策略的技能，这些策略用于启动进出用户网络的安全访问。申请者还应该能够监视网络上与安全有关的活动，并且采取措施阻挡入侵者对网络的攻击。

获取CCSA的第一步是获得有关方面的推荐，以证实拥有6个月的VPN-1/FireWall-1使用经验。此后，申请者可以参加Exam 156-210: VPN-1/FireWall-1 Management I NG考试。该考试将考核以下方面：

- 管理安全策略以及进行安全策略故障诊断的能力
- 测试并提高VPN-1/FireWall-1的性能
- 生成网络对象和组
- 记录管理操作的能力
- 配置防欺骗防火墙，以防止入侵者访问网络
- 生成用户和组，并且针对用户、客户和会话身份验证进行实施
- 配置网络地址翻译（静态NAT和隐藏NAT）
- 对VPN-1/FireWall-1进行备份
- 卸载VPN-1/FireWall-1

申请者成功地通过了VPN-1/FireWall-1 Management I NG考试后，就可以获得CCSA证书，然后能够继续申请Check Point公司的其他认证。

Check Point认证安全专家

在参加Check Point认证安全专家（Check Point Certified Security Expert，CCSE）考试（Exam 156-310）之前，应试者应该具备配置以VPN-1/FireWall-1为中心的因特网安全解决方案的知识和技能，还应该具备配置虚拟专用网络（Virtual Private Networks，VPN）的能力。CCSE认证建立在CCSA认证的基础上，因此申请者必须先通过CCSA考试，然后再参加CCSE考试。应试者在配置内容安全保护、设置用户定义的追踪措施以及保护系统不受大量的SYN信息攻击等方面的能力将经受检验。

Check Point公司要求申请CCSE认证的人员具有一定程度的熟练技能。除了必须掌握CCSA所要求的技能之外，申请者还必须能够完成下列工作：

- 使用扫描和访问评估工具查找系统存在的弱点，然后再修改自己的安全策略以封闭可能存在的任何漏洞。
- 能够制定一个安全网络体系结构，其中应该包含VPN和DMZ这样的组件，还要使用内容安全（Content Security）措施来过滤HTTP、SMTP、FTP和TCP信息传输。
- 安装VPN-1/FireWall-1并完成与之相伴的安装之前和安装之后的任务，如装入和固化操作系统。
- 能够编辑系统文件如smtp.conf和objects_5_0.C，还应该能够从自己的数据库中导入用户并向数据库导出用户。
- 能够在分布式环境中以及VPN-1/FireWall-1和OPSEC产品之间配置安全内部通信（Secure Internal Communications，SIC）。
- 能够使用日志以及像TCPDUMP这样的基本网络工具进行基本的故障诊断。
- 熟悉OPSEC伙伴以及它们与VPN-1/FireWall-1集成的能力。

说明： Sybex公司把《CCSE NG：Check Point认证安全专家全息教程》（CCSE NG: Check Point Certified Security Expert Study Guide（ISBN 0-7821-4116-1））一书作为CCSE考试（Exam 156-310）应试者的学习资料。如果想了解更多的相关信息，请查看网址www.sybex.com。

Check Point公司的其他认证

人们在获得了CCSE认证之后，都很想继续获取Check Point认证高级安全专家：企业集成和故障诊断（Check Point Certified Security Expert Plus: Enterprise Integration and Troubleshooting，CCSE Plus）资格。这是针对VPN-1/FireWall-1技术的最高级认证，需要申请者首先获得CCSA和CCSE认证。CCSE Plus认证可以证明其持有者具有Check Point公司VPN-1/FireWall-1技术的高级应用技能。这项认证要求其申请者具有丰富的故障诊断、网络规划以及实现复杂的VPN-1/FireWall-1配置的知识。为了获取CCSE Plus认证，申请者必须通过VPN-1/FireWall-1 Management I NG（Exam 156-210）考试、VPN-1/FireWall-1 Management II NG（Exam 156-310）考试和VPN-1/FireWall-1 Management III NG（Exam 156-510）考试。除了VPN/Security系列之外，Check Point公司还提供了另外两个认证系列：性能/可用性（Performance/Availability）系列和管理（Management）系列。

Check Point公司的性能/可用性（Performance/Availability）认证就是Check Point认证的服务质量专家（Check Point Certified Quality of Service Expert，CCQE）认证，该认证针对的是网络带宽管理。CCQE应该具备使用Check Point公司的FloodGate-1软件以及VPN-1/FireWall-1软件进行配置、实施和管理带宽策略的能力。如果想成为一名CCQE，申请者必须通过Exam 156-605: Quality of Service Using FloodGate-1（考试156-605：使用FloodGate-1实现服务质量管理）考试。

在管理（Management）系列中，Check Point公司提供了两项认证：Check Point认证寻址专家（Check Point Certified Addressing Expert，CCAE）和Check Point认证托管安全专家（Check Point Certified Managed Security Expert，CCMSE）。CCAE认证要求申请者具备在企业网络中实施和配置Check Point公司的Meta IP软件的能力，以及针对IP地址进行高效管理的能力。CCAE还必须能够配置和管理DNS和动态DNS（Dynamic DNS）。要想获得CCAE资格，申请者必须通过Exam 156-705: Introduction to Meta IP/Deploying and Troubleshooting Meta IP（考试156-705：Meta IP简介/Meta IP部署和故障诊断）考试。

CCMSE申请者必须要先获得CCSA认证和CCSE认证。获得了CCSE认证之后，申请者必须能够将VPN-1/FireWall-1作为企业安全解决方案，并且能够在网络操作中心（Network Operating Center）环境中部署Provider-1软件作为集中化的策略管理方案。CCMSE是Check Point公司各项认证中级别最高的。获得此项认证的人士完全有能力基于Check Point解决方案接受安全服务托管任务。

如果想获得CCMSE认证，申请者必须通过VPN-1/FireWall-1 Management I NG（Exam 156-210）考试、VPN-1/FireWall-1 Management II NG（Exam 156-310）考试以及Managing Multiple Sites with Provider-1 NG（Exam 156-810）考试。

如果读者想了解关于Check Point公司所提供的各项认证的进一步情况、更新信息和认证方面的新闻，请查看网址：www.checkpoint.com/services/education/certification/index.html。

说明：要记住，考试主题和考试内容可能会随时改变而不事先进行通知。请大家一定要查看Check Point公司的网站以了解最新信息，网址是www.checkpoint.com/services/education/certification/index.html。

考试地点

在世界上120多个国家中设有3300个以上的VUE考试中心（www.vue.com），在其中任何一个考试中心都可以参加考试。申请者不能通过电话进行注册，而只能在网上注册。申请者可以访问www.vue.com，单击IT Certification（IT认证），从认证列表中选择Check Point，再单击Go按钮。在这个网页（www.vue.com/checkpoint/）上，申请者可以进行VUE注册，并且选择一个与自己距离较近的考试中心。

为了进行Check Point认证安全管理员（Check Point Certified Security Administrator）考试注册，申请者可以按照下列步骤操作：

1. 生成自己的VUE用户名和密码，然后再进入。确定自己希望参加的考试号。
2. 在本地区距离最近的VUE考试中心进行注册。这时考试中心会要求申请者预付考试费。在编写本书的时候，考试费用为150美元。申请者可以预先安排考试时间，但如果想在考试当日申请的话，就必须直接给VUE考试中心打电话。如果一次考试未能通过，那么必须等到下一次才允许再次考试。如果出于某些原因申请者需要撤销考试约定并重新安排日期，那么必须在原定考试日的一个工作日之前与VUE取得联系。如果在原定考试日期之前不足24小时内要求撤销或者重新安排一项考试的话，则考试中心不会批准，并且仍然收取相应的考试费。即使申请者届时未能参加考试，他也必须支付考试费。
3. 在安排考试日期的时候，申请者会收到全部关于预约和撤销过程、身份证要求和关于考试中心地址的指示信息。

关于参加CCSA安全考试的提示

CCSA考试约有75道试题，要求来自澳大利亚、百慕大群岛、加拿大、日本、新西兰、爱尔兰、南非、英国或美国的考生在90分钟内完成。所有其他国家和地区的应试者则可以在120分钟内完成。应试者必须获得总分数的69%，其考试才及格。前面曾经谈到，大家在参加考试之前，一定要查看Check Point公司的网站以了解更具体的信息。

不论应试者是否已经通过了以往版本的VPN-1/FireWall-1考试，这里都没有升级考试。这里的考试不是自适应（adaptive）考试，题型包括多项选择和判断对错。要记住，一定要认真阅读每一道题。同时，不要忘记正确的答案是Check Point公司的答案。在许多情况下一道题会有多个合理的答案，但正确的答案则只有Check Point公司推荐的答案。不要在答案中过多地使用自己的常识和经验。

Check Point公司对于答错的题目不倒扣分，因此如果应试者不知道某道题的正确答案，可以写上自己猜测的答案。考试中的每个主题方面对应着本书中的一章，其中的试题都是从一个包含许多试题的题库中选取的。在考试中并不是每个考试目标都会以题目的形式出现，因此每次考试都不相同。试卷中还有一些问题选自一些具有共性的事件和Check Point公司的技术辅导中心（Technical Assistance Centers）遇到的问题。

认证的有效期最短为18个月，只要是针对目前发布的主要产品版本或者比当前版本更新的版本，就是有效的。

下面是我们为了使大家考试取得成功而提出的一些比较普遍的提示：

- 提前到达考试中心，以便于进行自我放松并复习学习材料。
- 认真阅读试题，不要急于做答。一定要保证自己准确地理解了每一道题所提出的问题。
- 在回答自己无法确定的多项选择题时，可以使用排除法先剔除明显错误的答案。这样做可以大大提高猜测出正确答案的概率。
- 在考试的过程中，应试者可以先做后面的题，然后再返回试卷前面完成相应的问题。应试者也可以在试卷上做标记，以便对自己无法确定的答案稍后再做定夺。我们发现这是一种很有效的办法，因为有时试卷中后面的内容会唤起应试者的一些记忆，从而使他找出前面做过标记的试题的正确答案。

考试结束后，应试者立刻就能够在线获得关于自己考试是否合格的通知，还有一份打印出来的考试分数报告（Examination Score Report），其中会指出该应试者的考试是否及格，以及试卷各部分所得的分数（考试管理员会向应试者提供打印的分数报告）。如果考试合格了，该申请人会在4周到6周内收到来自Check Point公司的确认通知信件，其中会说明申请人获得的这项认证将能够带来的收益，还有可以用来访问Check Point公司SecureKnowledge网站的用户名和专业人员标识号（Professional ID）。密码将通过电子邮件发送过来。

关于作者

Justin Menga获得了Check Point认证安全专家（CCSE）资格和Cisco认证网际互联专家（Cisco Certified Internetworking Expert，CCIE）资格，目前在新西兰Logical Networks Ltd.公司担任网络设计顾问。这是一家全球性质的网络集成公司。此前，Justin曾经在康柏电脑公司从事网络解决方案设计师的工作。

Justin目前的工作是为使用大型企业网络的客户提供网络和安全设计/顾问方面的服务。如果读者希望与Justin联系，可以发电子邮件到jmenga@hotmail.com。

评估考试

1. What are the minimum rights required to block intruders?
   A. Read-only access to the Log Consolidator component
   B. Read-write access to the Log Consolidator component
   C. Read-only access to the Monitoring component
   D. Read-write access to the Monitoring component

2. Which of the following describes the information on which control decisions can be made using stateful inspection? (Choose all that apply.)
   A. Application-derived state.
   B. Evaluation of flexible expressions based on application-derived state, communication-derived state, and communication information.
   C. Application-layer proxying.

D. Inspection of Layer 2 parameters.

E. Connection table.

3. Which of the following protocols is compatible with hide NAT? (Choose all that apply.)

A. ICMP

B. IPSec

C. TCP

D. UDP

4. Which of the following applications can be used to configure security objects? (Choose all that apply.)

A. SmartDashboard

B. SecureUpdate

C. System Status

D. Visual SmartDashboard

5. What is the quickest way to only view accounting log entries in Check Point NG?

A. Use the Account log mode

B. Use the Audit log mode

C. Use the Account predefined log query in log mode

D. Apply a log query to the Type field including only accounting log entries

6. You are using SmartView Status to monitor an enforcement module, and you notice a status of Untrusted on the FireWall-1 module. What is the most likely cause?

A. SIC has not been established with the enforcement module.

B. The FireWall-1 services on the enforcement module have failed.

C. No security policy is installed on the enforcement module.

D. The network connection to the enforcement module has gone down.

7. Which of the following *best* describes the function of a firewall?

A. Provides address translation to connect the internal network to the Internet.

B. Provides stateful inspection to ensure secure remote access communications.

C. Protects the internal network from the Internet.

D. Protects the internal network from external customers networks.

8. You hide a rule in your security rule base and install the rule base onto an enforcement module. Which of the following statements is *not* true?

A. The hidden rule is displayed as a gray line in SmartDashboard.

B. The hidden rule is not enforced by the enforcement module.

C. The hidden rule can be displayed by selecting Rule➤Hide➤Unhide all.

D. The hidden rule is logged in the security log if the tracking option is set to log.

9. What are the advantages of stateful inspection over other firewall types? (Choose all that apply.)
   A. Provides filtering of Layer 3 and Layer 4 parameters.
   B. Combines the performance of a packet filtering firewall with the security and application awareness of an application-layer gateway.
   C. Protects clients by proxying connections on behalf of clients.
   D. Cheaper than other firewall types.

10. Which of the following is true regarding implicit client authentication? (Choose all that apply.)
   A. It is the same as partially automatic client authentication.
   B. Users must manually authenticate to the TELNET or HTTP security server.
   C. Users can authenticate via user authentication to authorize the client authentication rule.
   D. Is the same as fully automatic client authentication.

11. What is the recommended memory requirement for a VPN-1/FireWall-1 NG enforcement module?
   A. 16MB
   B. 64MB
   C. 128MB
   D. 256MB

12. Which of the following authentication types are transparent from a users perspective? (Choose all that apply.)
   A. User authentication
   B. Client authentication
   C. Implicit client authentication
   D. Session authentication

13. Which of the following describes the term client side? (Choose all that apply.)
   A. When a packet is transmitted out of an interface
   B. When a packet is received on an interface
   C. Where source NAT is performed
   D. Where destination NAT is performed

14. Where does the ICA reside?
   A. Enforcement module
   B. Management client
   C. Management server
   D. External CA

15. What are the two types of Check Point NG licenses?
    A. Central
    B. Local
    C. Remote
    D. Distributed

16. What are the functions of an enforcement module? (Choose all that apply.)
    A. Store the user database.
    B. Authenticate users.
    C. Maintain security logs of traffic.
    D. Inspect traffic against a security rule base.
    E. Provide network address translation.

17. You attempt to install a policy onto a remote enforcement module from a management server. You get a connection timeout error. You can still access the Internet from a PC via the enforcement module. What is the *most likely* cause of the problem?
    A. SIC is not established with the enforcement module.
    B. The implied VPN-1 control connections rule has been disabled.
    C. The Check Point enforcement module service has crashed.
    D. The stealth rule is applied too high in the security rule base.

18. A customer phones you, complaining that he has configured automatic NAT for a security object, added the appropriate security rules, and installed the policy; however, external devices using the rule can't connect to internal devices configured for automatic NAT. The customer has checked the ARP cache of his border routers and verified that the correct MAC address is associated with the valid IP address configured for automatic NAT. Which of the following could be the cause of the issue? (Choose all that apply.)
    A. The customer has configured hide NAT for the object.
    B. The customer has disabled automatic ARP.
    C. The customer has configured static NAT for the object.
    D. The customer has disabled client-side destination translations.

19. What are the default objects present in the users database? (Choose all that apply.)
    A. Default
    B. Default User
    C. Default Users
    D. All Users

20. An administrator wishes to block access using a security rule, with a notification

sent to the system attempting access. What action should be specified for the rule?

A. Accept

B. Deny

C. Encrypt

D. Reject

21. Which of the following types of NAT is required for enabling external devices to connect to internal devices with private IP addresses? (Choose all that apply.)

A. Destination NAT

B. Hide NAT

C. Source NAT

D. Static NAT

22. Which of the following requires backup on a SmartCenter server? (Choose all that apply.)

A. $FWDIR/bin

B. $FWDIR/conf

C. $FWDIR/lib

D. $FWDIR/state

23. You wish to configure anti-spoofing for the internal interface of your VPN-1 /FireWall-1 NG module. Three separate networks reside behind the inside interface. Which of the following must you do to define anti-spoofing? (Choose all that apply.)

A. Define the addresses behind the interface as External.

B. Define the addresses behind the interface as Internal.

C. Configure a group object that includes each of the internal networks.

D. Configure the addresses behind the interface as Specific.

E. Configure the addresses behind the interface as Defined by the interface.

24. Users on your network are complaining of slow Internet access to web sites. You narrow the problem down to your enforcement module. You notice that the web access rule has a rule number of 100, and that numerous anti-spoofing log messages are being generated. What should you do to rectify the problem?

A. Place the web access rule near the top of the rule base.

B. Configure a hosts file on the SmartCenter server.

C. Disable NAT rules.

D. Disable anti-spoofing.

25. What is the mechanism used by Check Point NG to ensure log unification?

A. Log ID