

CCSE NG: Check Point Certified Security Expert Study Guide

CCSE NG: Check Point

认证安全专家全息教程

考试号: 156-310

[美] Valerie Leveille 著
Sarvang Shah

钟林辉 陈爱国 张文耀 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



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

**CCSE NG: Check Point Certified
Security Expert Study Guide**

CCSE NG: Check Point 认证安全专家全息教程

〔美〕 Valerie Leveille 著
Sarvang Shah

钟林辉 陈爱国 张文耀 等译

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 提 要

Check Point是防火墙和VPN方面全球市场的领导者, Check Point提供了各种各样的认证级别, 以量化技术人员掌握的网络安全知识以及管理员使用Check Point产品实现网络安全的能力。本书提供了帮助读者通过Check Point认证的安全专家: VPN-1/FireWall-1 Management II-NG (156-310) 考试所需要的所有内容, 其中包括: VPN-1/FireWall-1的安装、负载平衡、内容安全、H.323和SIP、加密和VPN、外部网络管理配置等。其中每一章的开头都列出了详细的考试主题清单, 结尾处提供了针对每一章内容的复习题和答案, 以帮助读者巩固所学的知识。

本书适用于网络管理员、网络安全专业技术人员以及高校计算机专业高年级的学生和研究生。



Copyright©2003 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

本书英文版由美国SYBEX公司出版, SYBEX公司已将中文版独家版权授予中国电子工业出版社及北京美迪亚电子信息有限公司。未经许可, 不得以任何形式和手段复制或抄袭本书内容。

版权贸易合同登记号: 01-2003-1091

图书在版编目 (CIP) 数据

CCSE NG: Check Point认证安全专家全息教程/(美)勒维尔 (Leveille, V.) 著; 张文耀等译. —北京: 电子工业出版社, 2003.8

书名原文: CCSE NG: Check Point Certified Security Expert Study Guide

ISBN 7-5053-8887-8

I. C… II. ①勒… ②张… III. 计算机网络—安全技术—软件工具, Check Point—教材 IV. TP393.08

中国版本图书馆CIP数据核字 (2003) 第056688号

责任编辑: 春 丽

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: 20.75 字数: 530 千字

版 次: 2003年8月第1版 2003年8月第1次印刷

定 价: 35.00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公司将一如既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

感谢那些帮助我经受这个严峻考验的人们。

—Valerie Leveille

谨以此书献给我心中的天使——我可爱的妻子Nisha Shah

—Sarvang Shah

致 谢

没有Sybex公司团队（他们是Liz Burke、Heather O'Connor、Maureen Adams和Tiffany Taylor）的努力工作与耐心，就可能没有本书的诞生。因为我们不是经历了一两个不同的Check Point NG产品，而是三个。我认为本书差不多是写了两遍。

此外，感谢Intelligent Connections部门中那些谅解我的同事。我意识到辛苦从事这一耗时6个月的项目所需要的耐心，因此感谢我的合著者和朋友Sarvang Shah，他一直与我一起辛苦地工作着。在本书出版后，我们将出去吃寿司！感谢我们的技术编辑Alan Bailey和Gareth Bromley，他们的“挑剔”确实使本书更加出色。

感谢我所有的朋友，特别是Patti、Diane、Byron、Don和Amber，当我为了完成本书而谢绝与他们的聚会的时候，他们仍耐心地支持我。我真地想念你们大家，恨不得下周去过教堂之后就跑出去与你们共进午餐！

最后感谢上帝，感谢你在我实在想退缩并浪费掉整个夏季的时候给我耐心和决心，使我能够坐下来完成这一项目。如果没有你我真是无法完成这一任务！

—Valerie Leveille

本书的策划和开发涉及到许多人。我要感谢整个Sybex团队：Liz Burke、Heather O'Connor、Maureen Adams和Tiffany Taylor，当我们一章一章地编写本书然后升级并针对FP3再次重来的时候，他们辛勤地工作着并显示出了极大的耐心。

我还要感谢我的朋友和合著者Valerie Leveille，她在编写本书时均衡了繁重的工作和学校的时间表。感谢我们的技术编辑Alan Bailey和Gareth Bromley，他们使本书的写作得以顺利进行。

我要感谢那些与我写的那一部分有直接或者是间接关系的人们。我还要感谢我的朋友和家人，他们不停地邀请我共渡这个夏天。我很遗憾最终谢绝了他们的邀请。明年夏天我们将弥补回来！我要感谢我的父母和岳父母，他们一直试图围绕我的写作时间表安排家庭活动；感谢我的姐姐Angana Shah，她在生活的许多方面给我以鼓励；感谢我姐夫Falgun Patel博士，他总是在我们需要的时候及时出现。

最为重要的是，如果没有我深爱的美丽的妻子Nisha Shah，我将不会是今天这个样子。我要特别感谢Nisha持续不断地支持、忍耐和引导我。

—Sarvang Shah

译者序

安全——网络的生存之本，在当代网络经济生活中具有重要的战略意义。伴随计算机与通信技术的迅猛发展，网络攻击与防御技术交替发展，优秀的国际化产品纷纷进入中国的计算机安全市场，而目前网络安全存在的突出问题是人才稀缺。因此，在网络安全日益受到关注的时候拿起这本书不失为一种明智的选择。

作为Internet和网络安全以及VPN和防火墙市场上的行业佼佼者，Check Point提供的产品和解决方案遍布全球149个国家和地区。为了衡量Check Point管理员和工程师的技术水平，Check Point提供了一系列的认证培训与考试，以此量化其网络安全知识以及管理员使用Check Point产品实现网络安全的能力。在从事这些认证考试的时候，读者将逐步全面掌握网络安全方面的知识。

作为Check Point认证考试的辅导教材之一，本书将帮助读者获得Check Point安全专家认证考试所需的扎实基础，并帮助读者通过VPN-1/FireWall-1 Management II-NG (156-310) 考试。本书是专门为这一考试编写的教程，内容涵盖了：

- VPN-1/FireWall-1 NG的安装、设置、升级以及卸载；
- VPN-1/FireWall-1 NG的跟踪防御功能；
- 负载均衡；
- 内容安全；
- Check Point支持的VoIP及其协议H.323和SIP；
- 加密的基本概念与原理、虚拟专用网的原理与概念，以及传统模式下的VPN解决方案；
- 简化的VPN技术；
- 外联网的配置与管理；
- Check Point客户端到站点的VPN技术——SecuRemote；
- 安全客户端SecureClient、策略服务器以及无客户端的VPN技术；

本书共10章，每章都以VPN-1/FireWall-1 Management II-NG考试所涵盖的目标清单开始。为了帮助巩固所学内容，每章的结尾都附有考试要点、关键术语表和复习题。此外，本书选配的光碟中包含全新的Sybex应试准备软件、全真模拟题、电子抽认卡和本书的电子版。这些辅助学习手段和学习材料，有助于读者方便快速地掌握所学知识。

本书内容翔实，条理清晰，紧密结合考试要点（大纲）与管理实践。译者在忠于原文的基础上，力求保持原文的风貌。然而，由于水平有限且时间仓促，错误与不妥之处在所难免，恳请广大读者谅解，并欢迎批评指正。

本书由张文耀、钟林辉、陈爱国、叶茂盛、黄早亮、廖频、苏菲和饶莹等人共同翻译，最后由张文耀负责全书统稿。

简介

欢迎来到令人激动的Check Point认证天地！你已经拿起了这本书，因为你想要一些更好的东西：也就是一个更好的更加满意的工作。毫无疑问，你已经做了一个正确的决定。

Check Point认证能够加深你对网络安全如何在Check Point产品之外的领域工作的理解。例如，当前有超过300个产品通过诸如VoIP（Voice over IP）和LDAP（Lightweight Directory Access Protocol）之类的协议以及诸如网络地址翻译（Network Address Translation, NAT）和内容过滤之类的技术集成了VPN-1/FireWall-1。位于www.opsec.com的Check Point的安全开放平台（Open Platform for Security, OPSEC）是一个负责建立用于将来自第三方供应商的产品与Check Point产品结合起来的的基础。

当然这不会损害到Check Point认证，因为Check Point是防火墙和VPN方面全球市场的领导者，而且自1995年以来一直如此。按照Check Point站点的话说，Check Point的解决方案“通过一个有2500个认证伙伴的网络在149个国家销售、集成并提供服务”。为了确保机构团体能够测量Check Point管理员和工程师的技术水平，Check Point提供了各种各样的认证级别，以量化技术人员掌握的网络安全知识以及管理员使用Check Point产品实现网络安全的能力。获取任何一级Check Point认证都将使你成为一个CCP（Check Point Certified Professional，Check Point认证的专业人员），那将使你有资格使用受密码保护的认证专业人员（Certified Professional）站点。在那里你将能够找到从公众领域中无法获取的工具、可选的软件、心得以及其他信息。成为CCP的其他好处还有能够访问SecureKnowledge数据库、收到产品升级通知、使用有关的徽标和证书、收到研讨会和其他Check Point活动的邀请。有关CCP程序的详细情况，请访问www.checkpoint.com/services/education/certification/index.html。

在获取Check Point认证的过程中，你将逐步全面掌握网络安全方面的知识。每一个网络安全工作都将从这些知识中受益，这也就是Check Point认证最近流行起来的原因。

本书的使用

如果你想要掌握通过Check Point认证的安全专家考试（Check Point Certified Security Expert, CCSE）的扎实基础，那么本书就足够了。我们已经花费了好几百个小时编写本书，惟一的目的就是帮助你通过VPN-1/FireWall-1 Management II-NG（156-310）考试。

本书包含一些非常有价值的信息，了解本书的组织结构将有助于你最有效地使用学习时间。

为了从本书中获取最大的好处，我们推荐以下学习方法：

1. 立即按照指示参加评估考试（答案在该考试的后面）。如果你不能回答所有问题，没关系。这就是你为什么要购买本书的理由！认真阅读你答错的每个问题的解释，并注意相关材料来自哪些章节。这些信息将帮助你设计学习策略。
2. 仔细研究每一章，确保完全掌握每章开头列举的信息和考试目标。并请特别注意自

已在评估考试中弄错的内容所在的章节。

3. 如果没有Check Point VPN-1/FireWall-1设备和可用的软件，那么一定要仔细研究例子。
4. 回答与每一章关联的复习题（答案在每章的结尾处）。注意那些使你糊涂的问题，并重新学习本书那些相关的章节。请不要简单地跳过这些问题！请确保完全掌握了每一答案的理由。
5. 在练习考试（practice exam）中一试你的身手。练习考试包含在本书选配的光碟中。这些考试中的问题只出现在该选配光碟中。这些考试将使你全面了解到你在真实的VPN-1/FireWall-1 Management II-NG考试中所能够预期到的情况。
6. 使用本书选配光碟中的所有抽认卡进行自我测试。该CD中新的升级的抽认卡程序将帮助你准备VPN-1/FireWall-1 Management II-NG考试。那是非常好的学习工具！

提示：电子抽认卡可以在Windows计算机、Pocket PC或Palm设备中使用。

7. 一定要阅读每章结尾处的关键术语和考试要点清单。这些学习辅助将帮助你巩固记忆中的各章的要点；此外它们还可以作为一种快速复习在你进入测试中心之前提供帮助。

为了学习本书覆盖的点点滴滴的资料，你将不得不严格自律。尽力每天都预留同样的时间进行学习，并选择一个舒适安静的环境。如果努力了，你将惊奇地发现自己可以很快地学习这一材料。

如果遵循我们列举的步骤，并努力学习和练习复习题、CD考试和电子抽认卡，那么你想要不通过VPN-1/FireWall-1 Management II-NG考试都会很难。

本书覆盖的内容

本书覆盖了通过VPN-1/FireWall-1 Management II-NG考试所要求了解的所有内容：

- 第1章涉及VPN-1/FireWall-1所要求的安装准备工作、安装过程以及安装之后的任务。
- 第2章讨论两种防御选项。用户定义的跟踪（UserDefined tracking）允许使用定制的日志选项，而SYNDefender选项可以使自己免受SYN flood攻击。
- 第3章涉及负载平衡。这个Check Point选项允许防火墙管理员使用在防火墙中定义的逻辑服务器，在选定算法的基础上确定镜像服务器组中的哪个服务器将获得下一个连接。
- 第4章讨论内容安全（Content Security）功能。该功能在使用或者是不使用外部CVP或UFP服务器的情况下结合了智能过滤HTTP、SMTP、FTP和TCP通信的功能。
- 第5章概述了Check Point支持的两个VoIP协议：H.323和SIP。
- 第6章深入讨论了加密和VPN以及如何用VPN-1/Firewall-1部署传统VPN的问题。
- 第7章涉及一个新的称为简化VPN（VPN团体）的NG功能部件，该部件自动操作一个公司内部的大多数VPN配置。
- 第8章讨论外部网络管理的配置，那是一种半自动地配置你的公司与其他公司之间VPN的方法。

- 第9章介绍SecuRemote，这是一个软件客户机，用来配置客户机到防火墙的VPN，其中涵盖了软件客户机配置和防火墙配置。
- 第10章详细查看了被客户机到站点的VPN中配置和部署SecureClient、Policy服务器和VPN-1/FireWall-1的情况。SecureClient用做其所在计算机上的个人防火墙，而不管其是否处于公司防火墙外的公司网络中。
- 术语表是一个便利的关于Check Point和其他安全术语的资源，对于理解本书使用的一些比较晦涩的术语很有帮助。

每章的开头都是VPN-1/FireWall-1 Management II-NG考试所涵盖的目标清单。务必确保在学习章节内容之前阅读该清单。此外，每章的结尾都带有复习题，这是为了帮助你巩固所学内容而特别设计的。为了真正使你掌握技巧，请认真阅读每一个问题。如果可能的话，请学完一章就做复习题。

说明：Check Point NG软件是定期更新的。过去，Check Point发布服务组件，使用补丁程序和增强的代码改善当前的产品。对于NG，Check Point发布功能组件（Feature Packs, FP），功能组件不仅包含补丁程序，还提供重要的功能和代码改进。在写作本书时最新的FireWall-1版本是Check Point NG Feature Pack 3。由于其广泛的功能增强，这个版本应该是你部署的最低选择，本书就建立在该版本的部署基础上。

说明：你可能注意到我们在Windows 2000和Windows XP上都使用了Check Point NG Feature Pack 3。有些FP3屏幕可能看起来与你的不同，具体情况取决于你所使用的Windows操作系统。

选配光碟上的内容

我们尽力提供一些有用的工具，帮助你获得认证，你应该在你的工作站上加载下面所有的工具，并在为考试而学习的时候使用它们。

全新的Sybex应试准备软件

由Sybex专家开发的应试准备软件将训练你通过VPN-1/FireWall-1 Management II-NG考试。在该测试引擎中，你将找到本书的所有复习题和评估考试，外加两套全真模拟考试。模拟考试只有在选配光碟中才有。你可以参加评估考试，按章节或者是按主题对自己进行测试，完成练习考试，或者是参加随机生成的包含各种问题的考试。

用于PC、Pocket PC和Palm设备的电子抽认卡

为了准备考试，你可以阅读本书、尝试动手实验、研究每章结尾的复习题，并利用包括在本书和选配光碟中的练习考试。除此之外，你还可以使用选配光碟中包含的抽认卡。如果你能够做完这些难题并理解答案，那么你将知道自己已经为VPN-1/FireWall-1 Management II-NG考试做好了准备。

抽认卡包含150个问题，这些问题是专门为了打击你、确保你准备好了考试而编写的。在复习题、练习考试和抽认卡之间，你对考试的准备将越来越充分。

PDF格式的CCSE学习指南

Sybex在选配光碟中以PDF格式提供了CCSE学习指南。因此你可以在PC或者是便携电脑上阅读本书。该电子版对于那些需要旅行而又不想携带书本的读者以及那些更喜欢在计算机上阅读的读者很有帮助（Acrobat Reader 5也包含在选配光碟中）。

Check Point——简史

Check Point Software Technologies是在1993年由Gil Shwed、Marius Nacht和Shlomo Kramer创立的，随后迅速成长为Internet和网络安全以及VPN和防火墙市场上的行业佼佼者。当初的小软件公司已经成长为安全市场上一个国际性的领导者，员工超过1000，2001年的收入超过5亿美元。公司的全球总部位于以色列的Ramat-Gan，美国的运作基地位于加州的Redwood市。

针对诸如Check Point VPN-1/FireWall-1、Provider-1和FloodGate-1之类的产品（这些产品建立在安全虚拟网络（Secure Virtual Network, SVN）体系结构的基础上），Check Point不断更新其安全产品，为Internet和网络安全提供重要的解决方案。OPSEC合伙人联盟通过集成和互操作能力将Check Point的性能扩展到了超过325家最主要的公司。

自从1997年以来，Check Point每年都获得各种奖项。2000年10月Network Computing将其列为“十年内最重要的产品”的前10名之内。

Check Point VPN-1/FireWall-1已经在美国和国际间接受了无数的认证，满足全世界的政府和商业团体要求的严格安全标准。Check Point NG已经取得下列认证：

- 信息技术安全鉴定的通用标准（Common Criteria for Information Technology Security Evaluation, CCITSE或者是“通用标准”）。这是一组被U.S. National Security Agency/National Institute of Standards和其他13个国家的对等机构认可的鉴定标准。CCITSE是多个国家共同努力编写的，是以前的可信计算机系统鉴定标准（Trusted Computer System Evaluation Criteria, TCSEC或“橙皮书”）的后继者。CCITSE可以从下面的网址获取：www.radium.ncsc.mil/tpep/library/ccitse/。
- 联邦信息处理标准（Federal Information Processing Standard, FIPS）140-1 2级认证。这是由U.S. National Institute of Standards and Technology's (NIST) 和 Communications Security Establishment (CSE) of the Government of Canada实施的，指定了设计用来防止诸如黑客攻击和其他信息犯罪之类的潜在威胁的安全需求。FIPS的信息可以在www.itl.nist.gov/fipspubs/index.htm上找到。
- IT安全鉴定标准（IT Security Evaluation Criteria, ITSEC E3），这是由英国的通信电子安全组（Communications Electronics Security Group, CESG）授予的，等价于标准Common Criteria EAL 4。更详细的信息请访问www.cesg.gov.uk/assurance/iacs/itsec/index.htm。

Check Point VPN-1/FireWall-1安全认证

Check Point为其产品发起了许多认证。处理的第一批认证包括基于VPN-1/FireWall-1产品的Check Point Certified Security Administrator (CCSA)、Check Point Certified Security Expert (CCSE) 和CCSE Plus。此后,应试者可以晋级到产品FloodGate-1的Check Point Certified Quality of Service Expert (CCQE)、产品Meta IP的Check Point Certified Addressing Expert (CCAE)。最后,Check Point为那些实现VPN-1/FireWall-1和Provider-1 Internet安全解决方案的人员提供了高级的Check Point Certified Managed Security Expert (CCMSE)。这一考试要求通过CCSA、CCSE以及使用Provider-1管理多个站点(Managing Multiple Sites with Provider-1)的考试。认证有效期至少为18个月。如果它们是针对当前主要的产品发布,或者刚好是比当前发布先进的产品发布,则被认为是最新的。

Check Point认证的安全管理员 (CCSA)

Check Point认证的安全管理员 (Check Point Certified Security Administrator, CCSA) 是基本认证,验证应考者配置并管理FireWall-1基本实现的能力。在参加该认证之前,你应该具有定义并配置安全策略、允许网络进出安全访问的技能。你还应该能够监视网络安全活动,采取措施阻击访问网络的入侵者。

获取CCSA认证的第一个步骤是参加Check Point授权培训中心 (Check Point Authorized Training Center) 的动手培训。多次参加培训在精力上或者是经济上都是不太可能的,所以本教程就是下一步的最好帮助。甚至在参加了培训或者是学习了本书之后,Check Point还建议进行6个月的VPN-1/FireWall-1使用体验。Check Point的产品有非常多的细微差别,以致没有人能够一次就了解到所有的。为了熟悉产品内部的工作方式,必须在一个有规律的基础上使用防火墙。此后,应考者可以参加考试156-210: VPN-1/FireWall-1 Management I-NG。将对CCSA应考者测试以下内容:

- 管理安全策略并排除其故障
- 测试并改进VPN-1/FireWall-1的性能
- 创建网络对象和组
- 记录管理操作
- 配置在防火墙上的反电子欺骗,防止入侵者访问网络。
- 为用户、客户端和会话鉴别创建用户和组。
- 配置网络地址转换 (Network Address Translation, NAT) (静态NAT和隐含的NAT)
- 备份VPN-1/FireWall-1
- 卸载VPN-1/FireWall-1

成功通过VPN-1/FireWall-1 Management I-NG考试的应考者将被授予CCSA,可以继续获取其他有价值的Check Point认证。

说明: Sybex提供“CCSA NG: Check Point Certified Security Administrator Study Guide (ISBN 0-7821-4115-3, 中文版《CCSA NG: Check Point认证安全管理员全志教程》已由电子工业出版社出版)”作为CCSA考试(考试号156-210)的准备解决方案。详细情况请访问www.sybex.com。

Check Point安全专家 (CCSE)

在参加Check Point Certified Security Expert (CCSE) 考试(考试号156-310)之前,你应该拥有将VPN-1/FireWall-1作为Internet安全解决方案来配置的知识 and 专门技术,以及配置虚拟专用网(VPN)的能力。CCSE认证建立在CCSA认证的基础上,因此,在参加CCSE考试之前必须通过CCSA考试。该考试将测试你配置内容安全(content security)、建立用户定义的跟踪、防止SYN flood以及其他相关事情的能力。

Check Point对CCSE认证要求一定的熟练程度。除了掌握CCSA要求的技能外,你还必须能够处理以下事情:

- 使用扫描和网络访问工具查找弱点(weaknesses),然后修改安全策略(Security Policy)封闭所有漏洞。
- 能够使用VPN和DMZ之类的组件定义安全的网络体系结构,使用内容安全(Content Security)过滤HTTP、SMTP、FTP和TCP传输。
- 安装VPN-1/FireWall-1,并执行与安装有关的安装前后的任务,例如加载固化操作系统。
- 能够编辑类似smtp.conf和objects_5_0.C的系统文件,同时从数据库中导入和导出用户。
- 在分布式环境以及VPN-1/FireWall-1和OPSEC产品之间配置安全的内部通信(Secure Internal Communications, SIC)。
- 使用日志和基本的网络工具,例如TCPDUMP,进行基本的故障诊断。
- 熟悉OPSEC合伙人以及他们集成VPN-1/FireWall-1的能力。

其他Check Point认证

一旦获取了CCSE,你将感到很有必要晋级到Check Point Certified Security Expert Plus: Enterprise Integration and Troubleshooting (CCSE Plus) 认证。这是VPN-1/FireWall-1最高级的认证。该认证建立在CCSA和CCSE认证的基础上。CCSE Plus认证将深入验证使用Check Point的VPN-1/FireWall-1的专门技术知识。该认证要求掌握故障诊断、网络规划并实现复杂的VPN-1/FireWall-1配置的广泛知识。为了获得CCSE Plus,应考者必须通过VPN-1/FireWall-1 Management I-NG(考试号156-210)、VPN-1/FireWall-1 Management II-NG(考试号156-310),以及第三个考试:VPN-1/FireWall-1 Management III-NG(考试号156-510)。除了VPN/Security Track:之外,Check Point提供了另外两个认证轨道:Performance/Availability和Management。

Check Point的Performance/Availability认证是Check Point Certified Quality of Service Expert (CCQE),该认证集中在网络带宽的管理上。CCQE要求使用Check Point的FloodGate-1软件和VPN-1/FireWall-1软件配置、实现并管理带宽策略。为了成为CCQE,应考者必须通过考试156-605: Quality of Service Using FloodGate-1。

在管理轨道中,Check Point提供了两个认证:Check Point Certified Addressing Expert (CCAIE)和Check Point Certified Managed Security Expert (CCMSE)。CCAIE认证要求具备在公司网络中实现并配置Check Point的Meta IP软件并简化IP地址管理的能力。CCAIE

还必须能够配置并管理DNS和动态DNS。CCAE身份的获取必须通过考试156-705: Introduction to Meta IP/Deploying and Troubleshooting Meta IP。

CCMSE应考者必须首先成为CCSA和CCSE。在获得CCSE之后,应考者还必须能够实现作为企业安全解决方案的VPN-1/FireWall-1,并将Provider-1软件作为一个集中的策略管理解决方案在网络运行中心(Network Operating Center)这样的环境中部署。CCMSE是最受尊敬的。他们是管理基于Check Point解决方案的主要专家。

为了获得CCMSE认证,应考者必须通过VPN-1/FireWall-1 Management I-NG(考试号156-210)、VPN-1/FireWall-1 Management II-NG(考试号156-310)以及Managing Multiple Sites with Provider-1 NG(考试号156-810)。

更多的有关Check Point的认证礼物、更新以及认证消息,请访问<http://www.checkpoint.com/services/education/certification/index.html>。

说明:请记住测试主题和测试都可能在没有通知的情况下发生改变。请经常访问Check Point网站,获取最新的信息(www.checkpoint.com/services/education/certification/index.html)。

到哪里参加考试

可以在120多个国家内超过3300个授权的VUE测试中心的任何一家参加考试(www.vue.com)。打电话不能登记考试,因为那将要求你在网上登记。进入www.vue.com,单击IT Certification,从认证清单中选择Check Point Software,单击Go。在结果页面(www.vue.com/checkpoint/)中你就可以注册VUE,并向你附近的考试中心提出考试申请。

登记Check Point Certified Security Expert考试的步骤是:

1. 创建你的VUE用户名和密码,然后签到。确定所要参加考试的号码。
2. 在最近的VUE考试中心注册。要求应试者预先支付考试费。在编写本书时的考试费是150美元。
3. 在预约考试的时候,你将收到有关约定程序和取消程序、所要求的身份证件以及考试中心位置等指导信息。简而言之,你可以预先确定考试时间。但是如果你要在当天考试,则必须直接给VUE考试中心打电话。如果考试没通过,则必须等到允许你再次参加的第二天才行。如果你有别的事情而需要取消或者是重订考试时间,那么请在你的考试约定之前的上班时间内与VUE联系。取消或重新安排考试提前的时间如不足24小时,将被认为是同一天而遭受被没收考试费的对待。考试费不会因应试者不到场而退回。

参加CCSE考试的提示

CCSE考试包含大约75道题。如果应考者是来自澳大利亚、百慕大、加拿大、日本、新西兰、爱尔兰、南非、英国或者是美国等地的话,则必须在90分钟内完成。如果应考者是来自所有其他别的国家或地区则被分配120分钟的时间。必须获得69%的得分才能通过考试。就像前面所说的,在参加考试之前,请查看Check Point的站点获取有关的具体情况。

即使你经过了前一版本的VPN-1/FireWall-1认证,也并没有升级考试。考试不是自适应的,有多项选择和正误判别题组成。请记住要仔细阅读每一道题。此外,正确的答案是Check

Point的答案。在很多情况下，给出了多个适当的答案，但是正确的答案指的是Check Point推荐的那个。不要让常识和经验影响你的回答。

Check Point不会为因不正确的答案而减分，因此即使不知道答案，也请给出你最好的推测。每一个主题领域（它对应于本书的章节）的问题都是从一个题库中抽取的。并不是每一个目标都出现在考试中，因此每一次考试都是独特的。考试还包含一系列从普通事件和Check Point Technical Assistance Center遇到的问题中提取的试题。

下面是一些考试成功的常规提示：

- 早点儿到达考试中心，以便能够放松并回顾一下学习材料。
- 仔细阅读问题。不要急于下结论。一定要使自己确切明白每个问题所问的是什么。
- 在回答你不太确定的多项选择题时，请使用排除法，首先删除明显不对的答案。这样将极大地提高你的命中率，如果你需要进行有根据的推测的话。
- 在考试中可以前后跳跃。如果不能马上确定答案，你可以记下该问题以便回顾。我们发现这非常有帮助，因为考试后期的某些事情可能恰好触发了记忆中的某个东西，使你能够回答前面标记的问题。

在完成考试之后，立即就可以得到考试通过或者是失败的在线通知。一份打印的考试成绩报告单（Examination Score Report）将指出通过或失败的状态，以及分节的考试结果（考试管理员将给你打印的成绩报告单）。如果通过了考试，你将在4到6周内收到来自Check Point的确认信件，其中概述了你的认证带来的好处，以及你的SecureKnowledge站点用户名和专业ID。密码将通过电子邮件分发。

关于作者

Valerie Leveille是经过认证的Check Point、Nokia和RSA教师。在受雇于Michigan Oak Park的Intelligent Connections L.L.C.时，她为各类的顾客提供咨询服务。通过电子邮件levelhead@wideopenwest.com可以和Valerie联系。

Sarvang Shah是CISSP，同时也是认证的Check Point和Nokia的教师。Sarvang通过他的IT安全咨询公司Elite-1 Security, Inc.（www.elite1security.com）为美国密歇根州范围内的顾客提供安全咨询与培训。通过电子邮件sarvang@elite1security.com可以和Sarvang联系。

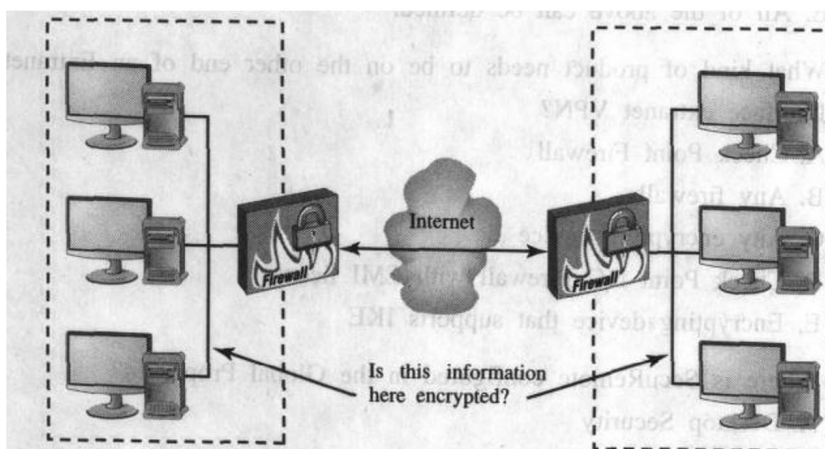
评估考试

1. What types of traffic can the Content Security feature filter?
 1. HTTP
 2. FTP
 3. AOL
 4. SMTP
- A. 1, 2
- B. 2, 3

-
- C. 3, 4
 - D. 1, 2, 4
 - E. All of them
2. Which command provides a menu for configuring the Check Point firewall?
- A. fwconfig
 - B. fwstart
 - C. cpconfig
 - D. fw putkey
 - E. fw putlic
3. Two rules are needed to implement HTTP load balancing.
- A. True
 - B. False
4. What does Secure Internal Communications (SIC) provide?
- A. A way for administrators to communicate with each other
 - B. A way for firewalls to perform health checks on each other
 - C. A point-to-point VPN between firewalls using IPSec
 - D. Secure communication between Check Point modules
 - E. A digital certificate authority
5. Where do you define alert scripts?
- A. In the Alert Commands tab of the Global Properties
 - B. In the Track element of the rule base
 - C. In the object properties
 - D. In the Visual Policy Editor
 - E. None of the above
6. To enhance security in a server-based VoIP solution, the server that the product is running on should have which of the following?
- A. Modem
 - B. Hard drive
 - C. Operating system
 - D. Hardened operating system
 - E. IP address
7. Persistent Server Mode should always be turned on.
- A. True
 - B. False
8. IPSec encrypts the payload and leaves the headers alone.
- A. True

- B. False
9. Which command is used to install a license in Check Point VPN-1/FireWall-1?
- A. fw printlic
 - B. cplic put
 - C. fw putlic
 - D. fw putkey
 - E. cp putlic
10. How many load balancing algorithms does Check Point support?
- A. 1
 - B. 2
 - C. 3
 - D. 4
 - E. 5
11. What process drives Check Point's Content Security features?
- A. Content Security daemon
 - B. fwauthd.conf
 - C. Security Servers
 - D. fwssd
 - E. CVP
12. What names are used for the Check Point component that must be installed prior to installing the firewall? (Choose all that apply.)
- A. CPOS
 - B. SVN Foundation
 - C. SecureOS
 - D. CPShared
 - E. IPSO
13. SMTP, FTP, and HTTP traffic can be filtered with Content Security without using an OPSEC server.
- A. True
 - B. False
14. What is the name of the Policy Server process?
- A. Policy.ps
 - B. dtps
 - C. psdt
 - D. cpd
 - E. None of the above

15. An SIP proxy is required to communicate via the SIP protocol.
- A. True
 - B. False
16. Which VoIP protocols are supported by Check Point NG? (Choose all that apply.)
- A. V.325
 - B. H.323
 - C. SIP
 - D. Real Media
 - E. Multi Media
17. SYN Relay completes the TCP/IP handshake with the server while waiting for the completed handshake from the client.
- A. True
 - B. False
18. Which Check Point product offers encryption but limited firewall functionality?
- A. FireWall-1
 - B. FireWall-1/VPN-1
 - C. VPN-1 Net
 - D. VPN-1 Pro
 - E. FloodGate
19. The information behind a firewall in a VPN is encrypted (see the following picture).



- A. True
 - B. False
20. ConnectControl is the same as load balancing.
- A. True
 - B. False