

Official Cert Guide

Learn, prepare, and practice for exam success



CCNP安全VPN 642-648 认证考试指南 (第2版)

[美] Howard Hooper, CCIE #23470 著
姚军玲, CCIE #11470 译



人民邮电出版社
POSTS & TELECOM PRESS

► 掌握CCNP安全VPN
642-648考试主题;

► 使用测试题评估各章知
识的掌握情况;

► 通过备考任务复习关键
概念;

利用CD-ROM中的模拟
试题进行练习。

Cisco职业认证培训系列
CISCO CAREER CERTIFICATIONS

CCNP安全VPN 642-648 认证考试指南 (第2版)

〔美〕Howard Hooper, CCIE #23470 著
姚军玲, CCIE #11470 译

人 民 邮 电 出 版 社
北 京

图书在版编目 (C I P) 数据

CCNP安全VPN 642-648认证考试指南 : 第2版 / (美)
豪柏 (Hooper, H.) 著 ; 姚军玲译. -- 北京 : 人民邮电
出版社, 2014. 9

ISBN 978-7-115-36530-9

I. ①C… II. ①豪… ②姚… III. ①计算机网络—安
全技术—工程技术人员—资格考试—自学参考资料 IV.
①TP393.08

中国版本图书馆CIP数据核字(2014)第176673号

版 权 声 明

CCNP Security VPN 642-648 Official Cert Guide (2nd Edition) (ISBN: 1587204479)

Copyright © 2012 Pearson Education, Inc.

Authorized translation from the English language edition published by Cisco Press.

All rights reserved.

本书中文简体字版由美国 Cisco Press 授权人民邮电出版社出版。未经出版者书面许可, 对本书任何部分
不得以任何方式复制或抄袭。

版权所有, 侵权必究。

-
- ◆ 著 [美] Howard Hooper CCIE #23470
 - 译 姚军玲 CCIE #11470
 - 责任编辑 傅道坤
 - 责任印制 彭志环 焦志炜
 - ◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
 - 邮编 100164 电子邮件 315@ptpress.com.cn
 - 网址 <http://www.ptpress.com.cn>
 - 北京艺辉印刷有限公司印刷
 - ◆ 开本: 800×1000 1/16
 - 印张: 41.25
 - 字数: 966 千字 2014 年 9 月第 1 版
 - 印数: 1—2 500 册 2014 年 9 月北京第 1 次印刷
 - 著作权合同登记号 图字: 01-2012-7080 号
-

定价: 118.00 元 (附光盘)

读者服务热线: (010)81055410 印装质量热线: (010)81055316
反盗版热线: (010)81055315

内容提要

本书是根据 Cisco 最新推出的 CCNP 安全 VPN 642-648 认证考试大纲要编写的考试指南。全书共分为 22 章和 2 个附录，详细阐述了 ASA 的架构，并对 Cisco 无客户端的远程访问 VPN、Cisco AnyConnect 远程访问 VPN、Cisco IPSec 远程访问 VPN、Cisco IPSec 站点到站点的 VPN 等常见的 VPN 技术的特点、配置和管理、验证和授权、高可靠性和性能等方面进行了详细的论述。本书还介绍了 Cisco 安全桌面的原理及实施，当用户通过 VPN 访问资源时，此技术可为用户提供一个非常安全的本地环境。

本书包含了大量的配置实例，并对 CLI 命令行和 ASDM 图形化界面分别进行阐述，有助于读者掌握配置方式和排错技巧。每章末尾的考试要点还可以帮助读者快速了解本章内容。

本书深入翔实地讨论与 CCNP 安全 VPN 考试相关的主题，能够帮助读者更好地备考 CCNP 安全认证考试。同时，从事网络安全工作的工程师、网络维护人员也可以从中受益。

关于作者

Howard Hooper, CCIE #23470、CCDA、JNCIA, 以网络顾问和培训师的身份供职于 **Transcend Networks** 公司, 致力于为企业客户和政府客户设计、安装和自动部署网络。他在网络行业已经工作了 10 年以上。在进入这个行当之初, 他作为一名技术支持工程师供职于一家服务提供商, 负责为中小型企业和服务提供商网络提供支持, 之后晋升为现场安装工程师和网络架构师。在其空闲时间, **Howard** 是一名专业的跳伞运动员和 Cisco 网络学院的讲师。如果他不是在跳伞, 那就一定是在本地的 Cisco 网络学院讲授 CCNA 课程。

关于技术审稿人

Chris Turpin, CCIE #17170, 是Tomorrows Networks公司的资深网络顾问。Chris在网络领域拥有15年以上的从业经验, 其专业技能横跨各种不同的技术学科, 其中包括IP电话通讯、安全、无线、LAN交换、数据中心网络和WLAN。最近, 他开始负责规划和设计跨越全球且具有安全性的大型IP和MPLS网络, 其中包括澳大利亚、欧洲和美国的网络。他还特别关注金融和服务提供商网络。他从纽卡斯尔大学获得了天文学和天体物理学的硕士学位。

Cristian Matei, CCIE #23684, 是罗马尼亚Cisco金牌代理Datanet公司的资深安全顾问。他设计、实施和维护的大型企业网络涵盖了Cisco安全、路由、交换和无线系列的产品。Cristian从2005年投身于网络行业, 主要从事Microsoft技术相关的工作, 并获得了MCSE安全和MCSE信息系统的认证证书。他随后加入Datanet公司, 并与不久之后就获得了CCIE安全认证, 以及注入CCNP、CCSP和CCDP在内的认证。从2007年起, Cristian成为一名Cisco认证的讲师, 开始讲解CCNP、CCNP和CCSP课程。在2009年, 他被Cisco公司评为“最被Cisco信任的技术顾问(TTA)”, 并获得了CICSP认证。同一年, 他开始作为技术编辑与其他网络专家合作编写CCIE路由&交换、安全的工作簿系列。在2010年, Cristian获得了ISACA认证的信息安全管理专家(CISM)证书。他当前正在准备路由&交换和服务提供商的CCIE认证。他还经常活跃在互联网专家和Cisco论坛上。

献辞

谨将本书献给我的家人和朋友。如果没有你们，我不可能取得今天的成就。

我要重点感谢下面这些人。

我的祖母 **Mary**，总是那么乐于奉献，乐于助人，并总会让我们如愿以偿，让我们无比快乐。迄今为止，我依旧非常想念您并且想念那些和您交谈的日子。我希望您为我感到骄傲，总有一天我们会再次相见。

我的继父 **Nigel**，是我见过的最勤奋和最博学的一个人，他也为我树立了做父亲的榜样。如果没有您，我不可能获得如今拥有的这些机会并拥有现在的这些知识。出于这些，我将永远对您心存感激。

我的姐姐 **Angela** 和姐夫 **Stuart**，你们一直陪伴在我的身边，并且以一种无人能想象的方式来帮助我。出于这些，我将永远感激你们并且希望有一天我能够回报你们的恩情。

我的儿子 **Ridley**，我希望有一天你能够理解我为什么不能总是和你呆在一起，尽管我内心是如此期盼！你的快乐在我心中弥足珍贵。爸爸想你并且非常爱你！

致谢

在本书写作期间，有些人一直身居幕后，并承担了大量的工作。在此，我想感谢每一位参与本书写作、审稿、编辑和出版的所有人。我要衷心感谢 **Brett Bartow**，他给了我写作本书的机会，并再三同意我延期交稿的请求，此外他还帮我克服了写作期间的很多障碍。我也要衷心感谢 **Eleanor Bru**，他和我一起孜孜不倦地工作，并成功将我的拙作“点睛”为当前看到的精品力作。写作很辛苦，而我又总是让他等待，因此，我要向他道歉，但是我非常感谢他，并且永远对他心怀感激之情。

我也必须向本书的技术审稿人 **Chris Turpin** 和 **Cristian Matei** 表达我的感激。你们的评审和建议对本书的质量大有裨益，也使得本书的内容更加完善。

最后，我要感谢我的家人，以及本书写作期间与之共事的所有人。没有你们，这一切都不可能发生。

前言

本书旨在帮助读者备考CCNP安全VPN认证考试。这门考试是CCNP安全认证考试中的其中一门。这门考试重点考查考生对Cisco IOS路由器、交换机和VPN设备应用安全原理的能力。

本书的读者

网络安全是一个复杂的课题。在你开始应用安全原理之前，应该先对计算机网络有一个深入的理解，并拥有丰富的经验，这至关重要。Cisco VPN课程旨在讲解与Cisco ASA和可用的客户端软件相关联的远程访问VPN和站点到站点VPN产品（这些产品也可能已经集成到Cisco ASA和客户端软件上），并解释它们是如何增强你的网络安全的。该课程主要面向网络管理员、网络安全管理员、网络架构师，以及经验丰富，且打算将安全原理应用到其网络的网络从业人员。

本书内容结构

本书分为22章，每一章都建立在前一章的基础之上。那些涵盖了命令和配置实例的章节也包含了相关案例的学习或者配置练习。

本书涵盖了如下主题。

- 第1章，“探讨VPN的角色和ASA所支持的技术”，本章讲解了VPN的操作原理和ASA的体系结构。本章是一个核心章节，为其他章节的学习打下了一个很好的基础。
- 第2章，“配置策略、继承和属性”，本章讲解了使用不同的方法来应用策略及其属性，以控制远程用户并且最终保护远程用户的连接。我们也引入了策略继承模型来帮助网络安全人员理解配置多种策略类型产生的效果。
- 第3章，“配置一个无客户端的SSL VPN解决方案”，本章讲解了Cisco无客户端SSLVPN的实施。除此之外，还讲解了如何配置一个基本的SSL VPN。
- 第4章，“高级的无客户端的SSL VPN的设置”，本章讲解了可用于无客户端SSL VPN部署的高级设置，以及访问应用程序的方法及其配置。
- 第5章，“定制无客户端的门户”，本章讲解了为远程用户定制无客户端的SSL VPN的环境时，可以使用的定制选项。本章还会讲解公共密钥基础架构（PKI）的实施和双因子验证机制。
- 第6章，“无客户端的SSL VPN的高级验证和授权”，本章讲解了组策略的实施和配置，以及其中包含的可用属性。本章还讲解了ASA可用的日志和计费方法。
- 第7章，“无客户端的SSL VPN的高可靠性和性能”，本章讲解了部署无客户端

的 SSL VPN 解决方案时，可以使用的 HA 和性能增强特性。

- **第 8 章，“配置 AnyConnect 远程访问 VPN 解决方案”**，本章讲解了 Cisco AnyConnect 远程访问 VPN 的配置和客户端软件。你将学到如何配置一个基本的 AnyConnect 远程访问连接，以及对一个远程用户进行验证所需的配置。
- **第 9 章，“AnyConnect VPN 的高级验证和授权”**，本章讲解了可用来对远程用户进行验证的验证机制。我们将进一步了解 PKI 技术和它作为一个独立的验证机制是如何实施的，还会讨论一起部署 PKI 和基于用户名/口令的验证方式时，需要完成哪些配置步骤（双因子验证）。
- **第 10 章，“AnyConnect 客户端的高级配置和管理”**，本章讲解了使用不同的方法来部署和安装 AnyConnect 客户端。除此之外，还探讨了各种不同的模块和它们的优点。
- **第 11 章，“使用 AAA 和 DAP 的 AnyConnect 高级授权”**，本章讲解了高级授权的角色和实施。高级授权允许我们对远程用户在 VPN 连接期间能够访问什么资源或者不能访问什么资源实施完全的控制。除此之外，本章还讲解了动态访问策略（DAP）的角色和如何使用它的配置来增强授权过程。
- **第 12 章，“AnyConnect 的高可靠性和性能”**，本章讲解了通过配置 AnyConnect 客户端或者使用外部硬件以满足在 ASA 设备上部署不同类型的冗余和高可靠性的需求。
- **第 13 章，“Cisco 安全桌面”**，本章讲解了 Cisco 安全桌面（CSD）的环境，以及在 AnyConnect 客户端和无客户端的 SSL VPN 中使用的相关模块。
- **第 14 章，“配置和管理 Cisco 的 VPN 客户端”**，本章讲解了 Cisco IPSec VPN 客户端和它的安装方法、配置方法以及高级的定制功能。
- **第 15 章，“部署 Easy VPN 解决方案”**，本章介绍了 Cisco Easy VPN 客户端和服务器的体系结构。除此之外，还讲解了配置一个基本的 Easy VPN、XAUTH 和 IP 地址分配等需要什么样的配置步骤。
- **第 16 章，“使用 Easy VPN 的高级验证和授权”**，本章讲解了 PKI 的配置和它在 Easy VPN 部署中的实施。本章也会讲解当证书映射被用于高级验证时，它所承担的角色。
- **第 17 章，“高级 Easy VPN 授权”**，本章讲解了组策略的实施和包含于组策略内的属性，它们可为远程用户提供高级的授权。除此之外，本章也讲解了日志和计费方法以及它们在 Easy VPN 部署中的用法。
- **第 18 章，“Easy VPN 的高可靠性和性能”**，本章讲解了可用来提供高可靠性（HA）解决方案的机制，它可以防止一个公司的 Easy VPN 的部署出现停机问题。
- **第 19 章，“使用 ASA 5505 作为硬件客户端的 Easy VPN 的操作”**，本章讲解了 ASA 5505 作为 Easy VPN 硬件客户端所具有的能力和如何配置硬件客户端。
- **第 20 章，“部署 IPSec 站点到站点的 VPN”**，本章讲解了在 ASA 设备上部署 IPSec

站点到站点的 VPN 解决方案和它的配置过程。

- **第 21 章，“IPSec 站点到站点的 VPN 的高可靠性和性能策略”**，本章讲解了为 IPSec 站点到站点的 VPN 部署提供硬件级别和软件级别的 HA 冗余机制。本章还讲解了 ASA 的服务质量机制(QoS)和与它相关的配置。
- **第 22 章，“最后冲刺”**，本章列出了学习过程中可以使用的备考工具，并提供了一个学习计划。
- **附录 A，“‘我已经知道了吗’ 测试题答案”**，本附录提供了每章开头“‘我已经知道了吗’ 测试题”的答案。
- **附录 B，“CCNP 安全 642-648 VPN 考试更新：版本 1.0”**，如果 Cisco 对编写本书所参考的考试大纲进行了少量的更新，那么本附录旨在帮助你获取这些更新内容。如果 Cisco 彻底改革了考试内容，本附录则无法涵盖所有变化的内容。那时，你将需要购买配套的新版认证书籍。更新的考试内容将会以 PDF 文件的形式发布在与本书配套的网站上：ciscopress.com/title/9781587204470。
- **术语表**，本术语表定义了出现在本章末尾的关键术语。在备考期间，你应该能够通过自己的理解去定义它们。

本书每章都具有相同的格式，并包含如下的工具来帮助你评估当前知识的掌握情况，并强化章节重点。

- **“我已经知道了吗？”测试题**：每章开头的一系列测试题将帮助读者检测对本章内容的熟悉程度。这些测试题根据章节重点进行划分，有助于你了解在学习本章时应当重点关注的地方。
- **基本主题**：作为每章的核心小节，基本主题给出了备考所需掌握的协议、概念及技能。
- **备考任务**：在每章的末尾，“备考任务”罗列了本章的考试要点。同时还给出了助记表附录和备考所需要的关键术语。不推荐为了通过认证考试而只关注本节所给出的考试要点、助记表和关键术语，但本节确实能够在最后备考冲刺阶段为你提供帮助。
- **CD 光盘上的考试练习**：本书配套的 CD 光盘上包含了一些免费的交互式考试练习。推荐使用这些练习进行考试前的自我测试。利用这些测试，你将熟悉最终的考试形式，并提高技能熟练程度。需要提醒的是，真正考试中的问题可能无法被预测。因此，你不能只是简单地着眼于“记住”每个可能的答案，而是应该通过扎实地学习来掌握课程重点，从而在考试中应对自如。

本书使用的图标





本章涵盖下述主题。

- 介绍虚拟私有网络：本小节将学习什么是 VPN，以及它可以在一个公司内外扮演的角色。除此之外，我们会讨论和比较用于 ASA 的不同的 VPN 方法。
- 满足 VPN 的协议：本小节介绍启动一个 VPN 连接所需的重要的协议，这些协议可以独立工作，也可以联合工作。当你学习本书的其余章节时，你可能想参考本小节来复习协议的特定细节。
- ASA 对数据包的处理：本小节将讨论 ASA 设备遵循的处理数据包的过程，即数据包通过 ASA 设备进入内部网络和一个数据包离开 ASA 去往外部网络的过程。
- 好的、坏的和许可证：本小节讨论被 ASA 采用的许可证模型，还有实施可选特性和不同的特性时所需的许可证需求。

目录

第 1 章 探讨 VPN 的角色和 ASA 所支持的技术	1
1.1 “我已经知道了吗？”测试题	1
1.2 介绍虚拟私有网络	3
1.3 支持 VPN 的协议	9
1.3.1 对称和非对称密钥算法	9
1.3.2 IPSec	10
1.3.3 IKEv1	10
1.3.4 验证头和封装安全负载	12
1.3.5 IKEv2	14
1.3.6 SSL/TLS	16
1.3.7 SSL 隧道协商	18
1.3.8 握手	19
1.3.9 DTLS	22
1.4 ASA 数据包处理	24
1.5 好的、坏的和许可证	26
1.5.1 基于时间的许可证	34
1.5.2 什么时候基于时间的许可证和永久许可证可被合并	34
1.5.3 共享的 SSL VPN 许可证	34
1.5.4 基于故障切换的许可证	35
1.6 复习所有考试要点	35
1.7 完成表格并通过记忆列出	35
1.8 定义关键术语	35
第 2 章 配置策略、继承和属性	37
2.1 “我已经知道了吗？”测试题	37
2.2 策略和它们的关系	38
2.3 理解连接配置文件	41
2.3.1 组的 URL	42
2.3.2 组的别名	42
2.3.3 证书到连接配置文件的映射	44
2.3.4 基于用户的连接配置文件的锁定	45

2.3.5 默认的连接配置文件	46
2.4 理解组策略	49
2.5 配置用户属性	51
2.6 使用外部服务器实现 AAA 和策略	53
2.7 复习所有考试要点	55
2.8 完成表格并通过记忆列出	55
2.9 定义关键术语	55
第 3 章 配置一个无客户端的 SSL VPN 解决方案	57
3.1 “我已经知道了吗？”测试题	57
3.2 无客户端的 SSL VPN 回顾	59
3.3 配置过程和策略	61
3.4 配置第一个无客户端的 SSL VPN 解决方案	62
3.4.1 IP 地址	63
3.4.2 主机名、域名和 DNS	63
3.4.3 成为一个公共密钥架构的成员	64
3.4.4 增加一个 CA 根证书	64
3.4.5 证书吊销列表	65
3.4.6 吊销检查	66
3.4.7 检索 CRL 的策略	67
3.4.8 检索 CRL 的方法	67
3.4.9 OCSP 规则	67
3.4.10 Advanced	70
3.4.11 为 SSL 启动相关的接口	78
3.4.12 创建本地用户账号用于验证	80
3.4.13 建立连接配置文件（可选的）	81
3.5 基本的访问控制	86
3.5.1 书签	87
3.5.2 HTTP 与 HTTPS	87
3.5.3 CIFS	87
3.5.4 FTP	88
3.5.5 组策略	90
3.6 内容转换	94
3.6.1 网关内容重写	94
3.6.2 Application Helper 配置文件	96
3.6.3 Java 代码的签名	97

3.7 对一个基本的无客户端的 SSL VPN 进行故障排查	98
3.7.1 对会话的建立进行故障排查	98
3.7.2 对有关证书的错误进行故障排查	100
3.8 复习所有考试要点	101
3.9 完成表格并通过记忆列出	101
3.10 定义关键术语	101
第 4 章 高级的无客户端的 SSL VPN 的设置	103
4.1 “我已经知道了吗？”测试题	103
4.2 回顾高级的无客户端的 SSL VPN 设置	105
4.3 通过端口转发访问应用程序	109
4.4 使用客户端/服务器插件的应用程序访问	115
4.5 通过智能隧道访问应用程序	123
4.6 配置 SSL/TLS 代理	129
4.6.1 邮件代理	129
4.6.2 内部的 HTTP 和 HTTPS 代理	131
4.7 对应用程序做故障排错	131
4.7.1 对应用程序的访问进行故障排错	132
4.7.2 客户端	132
4.7.3 ASA/VPN 终结设备	132
4.7.4 应用程序/Web 服务器	134
4.8 复习所有考试要点	135
4.9 完成表格并通过记忆列出	135
4.10 定义关键术语	135
第 5 章 定制无客户端的门户	137
5.1 “我已经知道了吗？”测试题	137
5.2 基本的门户布局配置	138
5.2.1 登录的定制	140
5.2.2 对门户页面进行定制	142
5.2.3 对登出页面的定制	143
5.3 对门户进行配置	144
5.4 门户语言的本地化	144
5.5 获取门户的帮助文件	148
5.6 AnyConnect 与门户的集成	149

5.7 无客户端 SSL VPN 的高级验证.....	151
5.8 为无客户端访问 VPN 使用一个外部和内部的 CA.....	152
5.9 无客户端的 SSL VPN 双因子验证	160
5.10 配置无客户端的 SSL VPN 的单点登录	164
5.11 对 PKI 和 SSO 的集成进行故障排错.....	168
5.12 复习所有考试要点	171
5.13 完成表格并通过记忆列出	171
5.14 定义关键术语.....	171
第 6 章 无客户端的 SSL VPN 的高级验证和授权	173
6.1 “我已经知道了吗？”测试题	173
6.2 配置过程、部署策略和信息收集.....	175
6.2.1 建立 DAP.....	178
6.2.2 指定用户的 AAA 属性.....	179
6.2.3 指定端点属性.....	180
6.2.4 配置授权参数.....	182
6.2.5 为默认的 DAP 配置授权参数	183
6.3 DAP 记录的集合	184
6.4 对 DAP 配置进行故障排查	189
6.4.1 ASDM 测试特性.....	189
6.4.2 ASA 日志.....	190
6.4.3 DAP 调试.....	191
6.5 复习所有考试要点	192
6.6 完成表格并通过记忆列出	193
6.7 定义关键术语.....	193
第 7 章 无客户端的 SSL VPN 的高可靠性和性能	195
7.1 “我已经知道了吗？”测试题	195
7.2 高可靠性的配置信息和常见的策略	196
7.2.1 故障切换.....	196
7.2.2 active/active	197
7.2.3 active/standby.....	197
7.2.4 VPN 负载均衡（集群）	198
7.2.5 外部的负载均衡.....	198
7.2.6 冗余的 VPN 对等体	198

7.3 缓存内容以实现优化	199
7.4 使用外部负载均衡设备实现无客户端的 SSL VPN 的负载均衡	201
7.5 为无客户端的 SSL VPN 的配置集群	202
7.6 对负载均衡和集群执行故障排查	204
7.7 复习所有考试要点	206
7.8 完成表格并通过记忆列出	207
7.9 定义关键术语	207
第 8 章 配置 AnyConnect 远程访问 VPN 解决方案	209
8.1 “我已经知道了吗？”测试题	209
8.2 AnyConnect 全隧道 SSL VPN 概述	212
8.3 配置过程、部署策略和信息收集	213
8.4 配置第一个全隧道的 AnyConnect SSL VPN 解决方案	215
8.4.1 IP 地址	215
8.4.2 启动 IPv6 访问	216
8.4.3 主机名、域名和 DNS	217
8.4.4 向 CA 登记并且成为 PKI 的成员	218
8.4.5 添加一个身份证书	218
8.4.6 添加签名的根 CA 证书	222
8.4.7 为 SSL/DTLS 和 AnyConnect 的客户端的连接启动接口	224
8.4.8 建立连接配置文件	225
8.5 配置第一个 AnyConnect IKEv2 VPN 解决方案	229
8.5.1 为 IKEv2 和 AnyConnect 访问启动相关的接口	230
8.5.2 建立 IKEv2 策略	231
8.5.3 建立连接配置文件	233
8.6 对客户端分配 IP 地址	236
8.6.1 使用连接配置文件分配地址	238
8.6.2 使用组策略分配地址	240
8.6.3 直接给用户分配地址	244
8.7 对环境的高级控制	245
8.7.1 ACL 和可下载访问控制列表	245
8.7.2 分离隧道	248
8.7.3 访问时长/时间范围	252
8.8 对 AnyConnect Secure Mobility 客户端进行故障排查	254
8.9 复习所有考试要点	259
8.10 完成表格并通过记忆列出	259