Cisco Systems

CCIE 职业发展系列
CCIE Professional Development

ciscopress.com

网络安全原理与实践

Network Security Principles and Practices

Expert solutions for securing network infrastructures and VPNs

[美] Saadat Malik, CCIE No. 4955 著
王宝生 朱培栋 白建军 译

人民邮电出版社
POSTS & TELECOM PRESS

CCIE 职业发展系列

网络安全原理与实践

[美] Saadat Malik，CCIE No.4955 著

王宝生　朱培栋　白建军　译

借　书　记　录

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

网络安全原理与实践/（美）马里克（Malik，S.）著；王宝生，朱培栋，白建军译.
—北京：人民邮电出版社，2003.8
ISBN 7-115-11318-1

I. 网… II. ①马… ②王… ③朱… ④白… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2003）第 043851 号

版权声明

CCIE 职业发展系列

网络安全原理与实践

◆ 著 [美] Saadat Malik, CCIE No.4955
译 王宝生 朱培栋 白建军
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
读者热线 010-67132705
北京汉魂图文设计有限公司制作
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：39.75
字数：961 千字 2003 年 8 月第 1 版
印数：1-3 000 册 2003 年 8 月北京第 1 次印刷

著作权合同登记 图字：01－2002－3722 号
ISBN 7-115-11318-1/TP・3480

定价：85.00 元

本书如有印装质量问题，请与本社联系 电话：（010）67129223

内容提要

本书为广大读者提供了安全网络设施和 VPN 的专家级解决方案。全书共分 9 个部分，分别介绍了网络安全介绍、定义安全区、设备安全、安全路由、安全 LAN 交换、网络地址转换与安全、防火墙基础、PIX 防火墙、IOS 防火墙、VPN 的概念、GRE、L2TP、IPSec 、入侵检测、Cisco 安全入侵检测、AAA、TACACS+、RADIUS、使用 AAA 实现安全特性的特殊实例、服务提供商安全的利益和挑战、高效使用访问控制列表、使用 NBAR 识别和控制攻击、使用 CAR 控制攻击、网络安全实施疑难解析等。附录中包括各章复习题答案和企业网络安全蓝图白皮书。

本书适合准备参加 CCIE 网络安全认证工作的人员，也适合那些想增强关于网络安全核心概念知识的网络安全专业人员。

关于作者

Saadat Malik（CCIE No. 4955）在Cisco系统的VPN和网络安全组管理技术支持工作。作为CCIE安全实验考试的作者、编写CCIE安全资格证书考试小组的成员之一，他是开发CCIE网络安全认证的先锋。目前他是CCIE的部门顾问，帮助改善正在进行的CCIE安全实验考试的质量。同时在监督CCIE实验考试方面，他有着多年的经验。过去，Malik在圣何赛州立大学教授研究生网络体系结构和协议的课程。这些年来，在Saadat的监督和技术领导下，30个CCIE（包括9个“double”CCIE和2个“triple”CCIE）已经达到了令人渴望的尊贵地位。多年以来，在业界的一些活动中，例如Networkers和IBM技术会议上，他经常就网络入侵检测相关的高级主题、VPN的疑难解析和高级的IPSec概念做报告。Saadat在West Lafayette（西拉法叶）的Purdue（波尔多）大学获得了电机工程硕士学位（MSEE）。

关于技术审稿人

Paul Forbes 是 Trimble Navigation 有限公司的高级网络工程师。他负责 Trimble 的全球 VPN、VoIP 和认证系统的开发和操作。他还活跃在入侵检测、无线和网络管理活动中。目前，在他能干的妻子的支持和辅助之下，他正在从事安全 CCIE 的工作。业余时间，他喜欢骑车和读书。

Randy Ivener 是 Cisco 公司高级服务小组的安全和 VPN 专家。他是认证信息系统安全专业人员、Cisco 认证网络专业人员、Cisco 安全专家 1 和 ASQ 认证软件质量工程师。几年来，他从事网络安全顾问的工作，帮助公司理解并负责他们的网络安全。Ivener 研究了很多安全产品和安全技术，包括防火墙、VPN、入侵检测和认证系统。在从事安全以前，他作为培训讲师进行软件开发工作。他毕业于美国海军学院，获得了工商管理硕士学位（MBA）。

Doug McKillip，进行 P.E.，CCIE 1851，是一名独立顾问，协助 Global Knowledge 公司（Cisco 系统的一个培训合作伙伴）Cisco 认证培训。在计算机网络方面他有 13 年以上的经验。在过去的 9 年里，他活跃于有关安全和防火墙方面的活动中。在 MCNS 版本 1.0 培训课程最初的开展中，Mckillip 提供了教学和技术辅导，并且是 Global Knowledge 公司的首席讲师和课程主管。他在 MIT 获得了化学工程学士和硕士学位，在 Delaware（特拉华）大学获得了计算机科学硕士学位。他居住在 Delaware 的 Wilmington（威尔明顿）。

献　辞

谨以此书献给：

我深爱的父亲 Hameed，

他用正确的信念、敏锐的原则和远见奠定了我的今天。

还有，

我亲爱的妻子 Alina，

她深深的鼓励、无限的耐心和慷慨的支持构筑了我们明天的美好生活。

致　谢

如果没有我在 Cisco 工作多年的同事们的指导和协助，本书是不可能完成的。为了完成本书，有很多人帮我做了大量工作。他们多年来一直不辞辛苦地勤奋工作，试图解决客户的问题，设计新的解决方案，提出客户最需要的正确答案。我从各个部门的同事们的工作中受益匪浅，尤其是 Cisco 系统的技术支持中心（Technical Assistance Lenter,TAC）。那里的确是未来领导人的摇篮。列出他们名字需要很长的篇幅，其中比较杰出的人是：Dianne Dunlap、John Bashinski、Natalie Timms、Wen Zhang、Frederic Detienne、Alok Mittal、Mike Sullenberger、Sujit Ghosh 和 Qiang Huang。他们只是那些对 Ciso 网络安全设计、实现和支持方面做出巨大有益工作的人们中的一部分。他们是从事并深刻理解网络安全领域的专家，是他们帮助我写出了你今天所看到的这本书。

此外，我还要特别感谢 Brett Bartow，本书的执行编辑。Brett 从我开始构思本书就一直支持、鼓励并指导我。他在我陷入众多职业和私人的事务时，在本书写作误期和滞后时给予了极大的理解，他使我能够坚持下去。我还要感谢在本书的最后阶段给我很大鼓励的开发编辑 Deborah Doorley，还有高级开发编辑 Chris Cleveland，在我需要的时候给予我帮助。

技术审稿人也审阅了本书。我要特别感谢 Randy Ivener，他非常仔细地审校了本书，指出了许多不足和缺点。本书也得到了 Randy、Paul Forbes 和 Doug McKillip 的大力帮助。

序　言

安全事件和影响网络、系统以及信息的攻击频繁地出现在技术性杂志和公众媒体上。自从 1988 年的 Morris 蠕虫事件至今，攻击事件的数量以每年超过两倍的速度随着 Internet 的扩张而增长。这些攻击事件包括为了识别网络设备和出现在网络上的服务而进行的扫描，对存在于这些系统和服务中的易受攻击设备或者服务的直接攻击，以及设计用于消耗带宽、CPU 或者其他资源的拒绝服务攻击。在过去的一年中，我们看到了大量严重的蠕虫病毒攻击，包括广为人知的红色代码（Code Red）和 Nimda 蠕虫病毒。据估计，红色代码蠕虫病毒造成的损失是 20 亿美元，并影响了成千上万的主机。这些蠕虫导致了拒绝服务攻击，并能够使攻击者完全地控制受害者的系统。在将它清除之后，又知道了微软的 Internet 信息服务（Internet Information Service，IIS）中的弱点，以及在攻击时有一个补丁可用。如果易受攻击的系统当时能够及时地打上补丁，那么蠕虫攻击所造成的大部分影响就可以避免。最近，在 Apache Web 服务器上出现了一种缓冲区溢出攻击，影响了大约 50%当时运行在 Internet 上的 Web 服务器。管理员为他们的系统打一次补丁需要多长时间？他们能在下一次大量的红色代码攻击到来之前打好补丁吗？挑战甚至是扭转这个趋势，要依赖技术供应商和设计、建设、维护当今复杂网络的专业人员。供应商必须提高他们产品的质量，负责系统和网络的专业人员必须将安全看成是他们网络基础结构中的一个重要和完整的构件。

本书对于从事网络安全工作的网络操作者和管理员来说是一个有价值的资产。不像是其他集中于某个单一安全技术（比如防火墙或者入侵检测系统）的书，本书列出了能够识别“什么时候”和“在哪里”的重要任务的位置，以便于定位一个网络内特定的安全技术。本书然后提供了涉及这些技术的具体配置信息。作者确保对配置作了详细的解释和经过了测

试，实例研究用于正确地使用理论知识。本书集中于深入协议级理解不同安全特性的功能。这是重要的，因为如果你只是肤浅地理解这些可用的特性和技术来为你的网络提供足够的安全性几乎是不可能的。网络安全当它真正需要的是一个可理解的、完整的方法时，时常被配置成一个解决方案要点的集合。这样的方法只有在专业人员对它的工作原理有一个深入的理解时才可能实现。

很高兴认识作者 Saadat Malik 已经有几年了。他是一个有天赋和有经验的网络专家，他的工作经验涉及本书所包括的所有领域。Saadat 作为 CCIE 安全实验考试作者的工作经历给了他 CCIE 网络安全认证所需的有判断力的眼光。这种眼光和洞察力使得本书成了那些 CCIE 安全认证工作者的一个有价值的资产。此外，他还有几年的时间是作为 Cisco 技术支持中心（Technical Assistance Center）的高级工程师，帮助客户解决与网络安全相关的疑难问题。他是网络安全方面的这个最终资源（指本书）的优秀作者。我强烈推荐本书作为每个从事安全领域工作的网络专业人员的必读书籍。

Barbara Fraser
Internet 工程任务组（IETF）IPSec 工作组，联合主席
Cisco 系统公司，总技术办公室，顾问工程师

前　言

本书主要提供对当今网络中不同安全规则、特性、协议和实现的深入理解。Cisco 安全实现是本书中讨论的不同主题的基础。本书的目的如下：

- 在较高的层次上提供一个对当今网络中涉及到的网络安全实现所有主题的讨论。
- 提供详细和深入的讨论，洞察协议背后网络安全实现的原理。
- 讨论形成不同网络产品、特性和实现基础的安全规则。
- 讨论者在提高网络安全性的网络设计的有用因素。
- 了解操作需求和设置要求，然后维持一个安全的网络。
- 讨论网络安全必需的网络维护和疑难解析技术。

本书的目标是提供一个对不同论题的高级讨论。但是，大部分论题从基础开始，以维持讨论的完整性。如果读者对网络安全相关的专业知识了解不多的话，这也能帮助读者更加容易地阅读本书。

本书假定读者已经熟悉基本的网络安全配置或者有 Cisco 命令参考手册，而避免详细地解释如何配置不同命令的排列。本书通过现实的实例研究解释了不同命令的用法，而不是独立地讨论它们。考虑到本书读者的水平，这些实例研究能够导致一些更有用的研究，而没有采用在命令参考中能读到的单个命令描述的形式。

本书面向的对象

本书主要面向两个群体：

- 没有学过 CCIE 或者学过 CCIE 的其他规范，而准备从事 CCIE 网络安全认证工作的人员。
- 可能已经完成了 CCIE 网络安全或者想增强关于网

络安全核心概念知识的网络安全专业人员。

本书涉及到大部分（如果不是全部的话）CCIE 网络安全测试的内容。通过提供关于安全协议、网络设计规则和指导方针的详细讨论，以及记录大部分普通设计要素，为 CCIE 应试者做了准备。本书的思想是为应试者提供在现实设计挑战中要遇到的问题和实现的结果。这样，当应试者在 CCIE 实验室考试看到类似的问题时，就能联系正确的上下文，并对所问的问题有一个深入的理解。这是任何应试者成功通过 CCIE 实验室测试的关键要素。

本书也面向那些对于增加网络安全不同方面知识感兴趣的网络安全专业人员。本书详细研究了有关网络安全要素比如防火墙和 VPN 设计的不同规则。在讨论不同的产品和技术解决现实问题真正实现之前，提供了这些产品和技术功能性的一个全面的基础和动机。本书涉及在不同协议中已经使用的高级特性，以及这些特性是如何解决复杂的网络和安全问题的。本书提供了对不同协议和算法工作原理的深入讨论。

本书的特点

本书是对安全规则及协议的研究和网络安全实现的一个组合。这都是必需的，因为尽管 CCIE 应试者需要理解配置是怎么工作的和实现是怎样完成的，但他们仍然要对底层的规则和协议是什么、列出的协议问题是什么有一个相当的了解。这是本书为什么讨论设计，以及为什么还要推荐基于协议和基于规则所涉及的不同要素描述的原因。如果读者想要对网络安全有一个全面的理解，而不考虑完成 CCIE 网络安全认证的话，这类分析也是有用的。

本书使用下面显而易见的特点以帮助读者在看完本书时达到想要理解的水平。

动机特点

本书在描述相关特性和更详细的内容之前，先讨论了为实现网络安全要素的不同方面的动机。这对于帮助读者获得不同的特性和规则的原理是非常重要的。

协议和产品实现分析

本书的一个主要侧重点是进入网络安全组的协议进行协议级讨论。本书也详细讨论算法（比如 PIX 的自适应安全算法）的实现。这些深入研究是构建读者宽广的专业知识结构所必需的内容。

所有配置、调试和 show 命令输出的逐行描述

本书的一个重要特点是逐行描述配置、调试输出和 **show** 命令的输出。这是帮助读者理解如何实现所讨论的不同特性的重要工具。

实例研究

本书使用了大量从现实世界中精选的实例，以进一步详细描述在本书中所讨论的设计和产品的特性。实例研究也是通过本书学习方案开发整体的一部分。大部分实例研究改编自 Cisco 的用户已经在他们的网络上实现了的实际情形。正因如此，它们是对于任何从事网络安全设计实现者的有用指导。

疑难解析

疑难解析是任何完整的网络安全实现的一部分。本书有一章详细描述所涉及的疑难解析的不同实现。第 24 章讨论疑难解析安全实现所需的技术和可用工具。也提供了大部分常见问题和配置错误的解决方法。

复习题和答案

大部分章节在最后部分都有“复习题”，它是一个有用的学习助手。复习题的答案在附录 A 中。

书中所用图标

贯穿本书，读者能够看到大量的图标用以指明 Cisco 和一般的网络设备、外设和其他项目。下面的图标注释解释了这些图标代表什么。

命令语法惯例

本书中所用的命令语法惯例与 IOS 命令参考中所使用的约定相同。下面给出命令参考中的惯例描述：

- 竖线（ | ）隔开多个相互独立的可选参数。

- 方括号（[]）表示可选参数。
- 大括号（{}）表示一个必需的选项。
- 方括号内的大括号（[{}]）表示在一个可选参数内必需的选项。
- **黑体**表示按所显示的逐字输入的命令和关键字。在实际的配置实例和输出（不是一般的命令语法）中，黑体表示用户手工输入的命令（例如一个 **show** 命令）。
- *斜体*表示需要读者提供实际值的参数。

目　录

第一部分　网络安全介绍

第二部分　构建网络安全