CISCO

ciscopress.com

网络安全原理与实践

CCIE Professional Development

Network Security Principles and Practices

Expert solutions for securing network infrastructures and VPNs

〔美〕 **Saadat Malik**, CCIE #4955 著
李晓楠, CCIE #23650 译

人民邮电出版社
POSTS & TELECOM PRESS

ciscopress.com

网络安全原理与实践

CCIE Professional Development

Network Security Principles and Practices

〔美〕 **Saadat Malik,** CCIE #4955 著
李晓楠, CCIE #23650 译

人 民 邮 电 出 版 社
北 京

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；李晓楠译. -- 北京 : 人民邮电出版社, 2013.8
ISBN 978-7-115-31243-3

Ⅰ. ①网… Ⅱ. ①马… ②李… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第105935号

版权声明

◆ 著　[美] Saadat Malik，CCIE # 4955
译　李晓楠，CCIE # 23650
责任编辑　傅道坤
责任印制　程彦红　杨林杰

◆ 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：42.75
字数：912 千字　2013 年 8 月第 1 版
印数：1－3 000 册　2013 年 8 月北京第 1 次印刷

著作权合同登记号　图字：01-2012-3994 号

定价：108.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书为广大读者提供了网络安全设施和 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、路由安全、局域网交换的安全、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阅读，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阅读。

关于作者

Saadat Malik，CCIE #4955，在 Cisco 公司负责 VPN 和网络安全小组的技术支持运维工作。作为 CCIE 安全实验考试的作者，以及编写 CCIE 安全考试小组的成员之一，他带头开发了 CCIE 网络安全认证考试。他当前是 CCIE 部门的顾问，为持续提升 CCIE 安全实验考试的质量而提供帮助。他在监考 CCIE 实验考试方面也有多年的经验。在过去，Malik 在圣何赛州立大学为研究生讲授网络体系结构和协议课程。多年以来，在 Saadat 的监督和技术指导下，已经有 30 多个持有 CCIE 认证（包括 9 个持有双 CCIE 认证的人员和 2 个持有三 CCIE 认证的人员）的人员取得了令人仰望的尊贵地位。最近几年，他还经常在行业会议上（比如 Networkers 和 IBM 技术会议）抛头露面，并就网络入侵检测、VPN 故障排错和 IPSec 高级概念等高级主题发表演讲。Saadat 在普渡大学西拉法叶校区获得了电子工程硕士学位（MSEE）。

关于技术审稿人

Paul Forbes 是 Trimble Navigation 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运营。他在入侵检测、无线和网络管理的倡议方面，也非常活跃。目前，在他的贤妻的支持和辅助之下，他正在准备 CCIE 安全方向的考试。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。他拥有 CISSP 认证（Certified Information Systems Security Professional）、CCNP 认证（Cisco Certified Network Professional）、Cisco 安全专家 1（Cisco Security Specialist 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，帮助公司理解并保护它们的网络安全。Ivener 接触过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。在从事安全工作以前，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，P.E.，CCIE #1851，是一名独立顾问，协助 Global Knowledge 公司（Cisco 公司的一个培训合作伙伴）的 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，他活跃于与关安全和防火墙相关的项目中。在 MCNS 版本 1.0 培训课程最初的部署中，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，在特拉华大学获得了计算机科学硕士学位。他居住在特拉华州的威尔明顿。

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。还将本书献给我的爱妻 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，本书几无问世可能。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 公司的技术支持中心（Technical Assistance Center，TAC）。那里的确是未来领导人的摇篮。受篇幅所限，这里不能将他们一一列出。其中比较杰出的人有 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 Cicso 网络安全的设计、实现和支持方面做出巨大贡献的部分人员。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，我还要特别感谢本书的执行编辑 Brett Bartow。Brett 从我开始构思本书就一直支持、鼓励并指导我。在我陷入众多工作和私人事务时，在本书写作误期和滞后时，他都给予了极大的理解，并让我坚持下去。我还要感谢本书的开发编辑 Deborah Doorley，是他的鼓励让本书成功收尾。我还要感谢本书的高级开发编辑 Chris Cleveland，他是我坚强的后盾。

本书的技术审稿人同样也功不可没。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。正是在 Randy、Paul Forbes 和 Doug McKillip 的大力帮助下，本书质量才得以进一步提升。

序

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。事实证明，在微软的 Internet 信息服务（Internet Information Service，IIS）中的漏洞暴露之后，也只有在攻击发生之后才有可用的补丁。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运维人员和管理员来说是一个宝贵的资产。与其他专门讲解某个单一安全技术（比如防火墙或者入侵检测系统）的图书不同，本书讲解了

一些重要任务，通过这些任务可以知道在什么时候，在网络的什么地方使用特定的安全技术。本书随后讲解了与这些技术相关的具体配置信息。作者在书中详细讲解了这些已经测试过的配置，并通过实例研究来帮助读者正确地使用书中讲解的理论知识。本书旨在从协议级别来深入讲解各种安全特性的功能。这很重要，因为如果你只是肤浅地理解了这些可用的特性和技术，也就无法为网络提供足够的安全性。在很多情况下，我们真正需要的是以一个全面、综合的方法来部署网络安全，此时就需要将单点解决方案（point solution）融合起来。如果你没有深入理解这些解决方案的运行机制，这种部署方式也就无从谈起。

很多年以前我就认识作者 Saadat Malik 了。他是一位相当有才华的资深网络专家，他的工作经验涉及本书讲解的所有领域。Saadat 是 CCIE 安全实验考试的作者，这使得他更为了解 CCIE 网络安全认证考试的要点。因此对有志于考取 CCIE 安全认证的读者来说，本书绝对是他们的宝贵学习资料。此外，他还以技术支持中心（TAC）工程师的身份在 Cisco 公司工作多年，其职责是帮助客户解决网络安全相关的问题。他是网络安全领域图书的最佳作者，对从事安全领域工作的网络专业人员来说，本书都是必读图书。

Barbara Fraser
Internet 工程任务组（IETF）IPSec 工作组，联合主席
Cisco 系统公司，首席技术办公室，咨询工程师

前　言

本书旨在帮助读者深入理解如今网络中实施的各种网络安全规则、特性和协议。本书使用 Cisco 安全实施作为讲解的基础，其目标如下所示。

- 在较高的层次上完整讨论了与实施网络安全相关的所有主题。
- 深入、详细地讨论了网络安全实施背后的协议运行机制。
- 讨论了构成不同网络产品、特性和实施基础的安全规则。
- 讨论以提高网络安全性为目标的网络设计的有用因素。
- 理解建立和维护安全网络的操作需求。
- 讨论网络安全必需的网络维护和故障排错技术。

本书旨在从较高的层次上讨论各种主题。但是，为了保持讨论的完整性，本书在讲解大部分主题时仍然是从基础开始的。这样，即使读者对网络安全相关的专业知识了解不多，也能更为容易地阅读本书。

本书假定读者已经熟悉基本的网络安全配置或者手边有 Cisco 命令参考手册，因此不会详细解释如何配置不同命令的排列。本书通过真实的案例研究来解释不通命令的用法，而非纸上谈兵。考虑到本书目标读者的水平，与 Cisco 命令参考手册简单罗列单个命令相比，这种案例式的研究会更有助于读者的学习掌握。

本书面向的对象

本书主要面向两个读者群体：

- 非 CCIE 人员，或者是持有其他方向的 CCIE 认证，当前正在备考 CCIE 网络安全认证的读者；

- 已经考取了 CCIE 网络安全认证，但是想进一步提升网络安全核心概念等知识的网络安全从业人员。

本书几乎涵盖了 CCIE 网络安全考试的所有内容。它为 CCIE 备考人员提供了各种安全协议、网络设计原理和指导的详细讲解，还提供了大部分常见设计元素的实施文档，其目的是为备考人员提供在实际的设计挑战和最终实施时面临的各种问题。这样，当备考人员在 CCIE 实验室考试中看到类似的问题时，就能够与合适的真实环境建立关联，从而深入理解问题的本质。这也是备考人员成功通过 CCIE 实验室考试的关键因素。

想要提升其网络安全知识的网络安全从业人员也是本书的目标读者。本书会详细讲解在设计网络安全组件（比如防火墙和 VPN）时，与之相关的各种规则。本书首先全面讲解各种安全产品和技术的基本功能和动机，然后讨论这些产品和技术在真实世界中的实施。本书涵盖了在不同协议中用到的高级特性，以及这些特性是如何解决复杂的网络和安全问题的。本书还详细讨论了各种协议和算法的运行机制。

本书的特点

本书不但研究了安全规则，还讲解了协议和网络安全实施等内容。之所以这样编排，是因为 CCIE 备考人员不但需要理解配置的工作机制和实施方式，还需要知道其底层的规则和协议是什么，正在解决的协议的症结是什么。这就是本书讨论不同网络元素的设计和建议，以及从协议和规则两方面描述网络元素的原因。如果读者知识想彻底理解网络安全，而不是仅仅为了通过 CCIE 网络安全考试，那么本书使用的这一分析类型也对你大有裨益。

本书使用下面的显著特点来帮助读者达到在看完本书时想要的理解水平。

动机特点

本书在讲解相关特性和深入讨论其内容之前，先讨论了实施网络安全元素的各种动机。这对于帮助读者深入理解不同的特性和规则的原理是非常重要的。

协议和产品实施分析

本书的一个主要特点是，对属于网络安全协议簇的协议进行协议级别的讲解。本书也详细讲解了算法（比如 PIX 的自适应安全算法）是如何实施的。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。

逐行描述所有配置、调试和 show 命令的输出

本书的一个重要特点是逐行描述配置、调试和 **show** 命令的输出。这是一个重要的工具，可以帮助读者理解所讨论的各种功能特性是如何实施的。

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 用户已经在他们的网络实施了的真实场景。正因如此，它们才正为网络安全设计实施人员的有用指导。

故障排除

故障排除是任何网络安全实施的不可分割的一部分。本书专劈一章来讲解各种实施的故障排除方法。第 24 章讨论了用来对安全实施进行故障排除的技术和工具，它还提供了大部分常见问题和配置错误的解决方案。

复习题和答案

本书大多数章节在末尾都有“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

在本书中，读者能够看到大量的图标，它们用来表示 Cisco 和一般的网络设备、外设和其他设备。下面的图标注释解释了这些图标所代表的意思。

命令语法惯例

本书命令语法遵循的惯例与 IOS 命令手册使用的惯例相同。命令手册对这些惯例的描述如下。

- **粗体字**表示照原样输入的命令和关键字，在实际的设置和输出（非常规命令语法）中，粗体字表示命令由用户手动输入（如 **show** 命令）。
- 斜体字表示用户应提供的具体值参数。
- 竖线（|）用于分隔可选的、互斥的选项。
- 方括号（[]）表示任选项。
- 花括号（{}）表示必选项。
- 方括号中的花括号（[{}]）表示必须在任选项中选择一个。

目　录