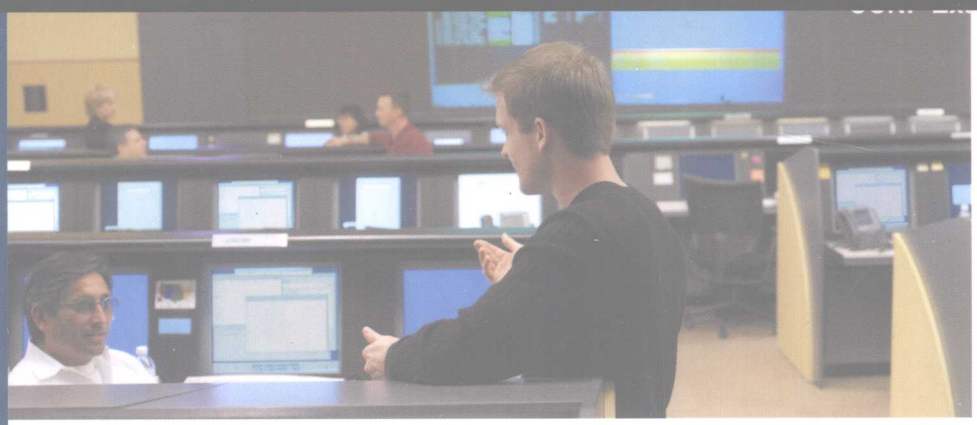
CCIE职业发展系列
CCIE Professional Development

ciscopress.com



网络安全技术与解决方案

Network Security Technologies and Solutions

A comprehensive, all-in-one reference for Cisco network security

〔美〕Yusuf Bhaiji，CCIE #9305 著
罗进文 王喆 张媛 饶俊 译

人民邮电出版社
POSTS & TELECOM PRESS

网络安全技术与解决方案

Network Security Technologies and Solutions

〔美〕Yusuf Bhaiji，CCIE #9305 著
罗进文 王喆 张媛 饶俊 译

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全技术与解决方案 /（美）海吉（Bhaiji, Y.）著；罗进文等译. —北京：人民邮电出版社，2009.3
(CCIE职业发展系列)
ISBN 978-7-115-19311-7

Ⅰ. 网… Ⅱ. ①海…②罗… 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（2008）第191151号

CCIE 职业发展系列

网络安全技术与解决方案

◆ 著 [美] Yusuf Bhaiji, CCIE #9305
译 罗进文 王 喆 张 媛 饶 俊
责任编辑 李 际
执行编辑 付 飞
◆ 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 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：787×1092 1/16
印张：37
字数：914 千字 2009 年 3 月第 1 版
印数：1－3 500 册 2009 年 3 月北京第 1 次印刷

著作权合同登记号 图字：01-2008-3326 号
ISBN 978-7-115-19311-7/TP

定价：79.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书是用于管理 Cisco 网络的综合性参考资料，能够帮助网络安全专业人士理解和实施先进的网络安全技术和解决方案。书中内容涵盖所有主要的 Cisco 安全产品、技术和解决方案，包括各种成熟的和新出现的技术信息，如自适应安全设备防火墙 8.0，Cisco 入侵防御系统感应软件 6.0，主机 IPS，Cisco 组加密传输 VPN，MPLS VPN 技术，Cisco 分布式拒绝服务异常检测和缓解方案，Cisco 安全监控、分析和响应系统，以及安全构架、标准和法规遵从性等。与主要关注概念与理论的图书不同，本书可作为配置和管理 Cisco 的领先动态链路的便捷工具书。

无论是对网络工程师或安全工程师、顾问，还是从事安全认证方面研究的读者，本书都是设计和构建安全网络的重要参考资料。此外，本书还为拟参加 CCIE 安全认证考试的读者提供了涵盖新大纲考点宝贵的备考资源。

关于作者

Yusuf Bhaiji，CCIE #9305（路由和交换与安全），已在Cisco公司工作了7年，现任Cisco CCIE安全认证的项目经理和Cisco Dubai实验室的CCIE代理人。此前，他曾是悉尼TAC安全及VPN团队的技术骨干。Yusuf对安全技术和解决方案的热情在他17年的行业经验中起着非常重要的作用，这从他最初攻读计算机科学硕士学位时就开始了，他毕业之后所获得的众多成就也证明了这一点。让Yusuf自豪的是他的知识共享能力，他已经指导了许多成功的考生，还在国际上设计和发表了许多网络安全解决方案。

Yusuf是几个非营利组织的咨询委员会成员，这些组织在Internet网络中发扬传统美德，通过学术和专业活动进行技术传播。Yusuf在巴基斯坦网络安全（NSP）和IPv6巴基斯坦论坛担任要职。

Yusuf还于2004年年初，通过Cisco出版社出版了一本名为《CCIE安全Lab实战》（已由人民邮电出版社翻译出版）的著作。他一直是Cisco出版社出版业务的技术评审，为之撰写文章、白皮书，并介绍各种安全技术。他还经常在一些会议和研讨会上进行著名的演讲。

关于技术审稿人

Nairi Adamian，CCIE 安全 No.10294，1999 年进入 Cisco 公司，目前是 Cisco 澳大利亚的技术支持经理。她在 Cisco 技术援助中心（TAC）领导一个客户支持工程师团队。她具有悉尼科技大学计算科学学士学位和 Macquarie 研究生管理学院的 MBA 学位。

Kevin Hofstra，CCIE No.14619，CCNP、CCDP、CCSP、CCVP。拥有耶鲁大学计算机科学学士学位和通信工程硕士学位，以及美国科罗拉多大学的工程管理硕士学位。

Gert DeLact，CCIE No.2657，是 Cisco CCIE 团队的产品部经理。Gert 作为一名作者对《CCIE Security 认证考试指南》和《CCDA 认证考试指南》（两书均已由人民邮电出版社翻译出版）做出了杰出贡献。他居住在比利时布鲁塞尔。

献　词

谨以此书献给我亲爱的妻子 Farah。如果没有她的支持和鼓励，我不可能完成这本书。

致　谢

我想感谢我的家人，因为他们的不断支持和鼓励，特别是我的父亲 Asghar Bhaiji，因为他的智慧。最后，也很重要，我怀念我的母亲 Khatija Bhaiji，她的爱永远照耀着我。

我特别要感谢技术评审，Nairi Adamian、Ger DeLaet 和 Kevin Hofstra，他们为本书做出了巨大贡献。他们在研究每一个主题时所提出的宝贵意见对本书的完善都非常有价值。

我真诚地感谢 Brett Bartow 和整个开发团队，包括 Betsey Henkels、Dayna Isley、Barbara Hacha、San Dee Phillips、Chris Cleveland 和参与这项工作的 Cisco 出版社团队的各位成员，他们的专业指导对本书的完成一直起着决定性作用。

我还想借此机会感谢我的经理 Sarab DeMark、Cisco 集团的领导和 Cisco 公司的同事们，感谢他们对本书写作及其他工作的支持。我已极大地受益于与他们一起工作，并很荣幸能成为这个团队的成员。最后，我想谢谢您——本书的读者——帮助我使这本书获得成功。

序

随着 Internet 经济的爆发式增长，关键任务系统的持续可用性已变得前所未有的重要。客户、员工和提供商都期望网络管理员和业务管理员能提供持续可用的网络资源，并能在一个完全安全的环境下访问关键应用和数据。这不仅仅是一个挑战，而且违反网络安全的代价也从未这样高过。

本书是一本用于管理 Cisco 网络，具有综合性、统一性价值的参考资料。编写本书的目的在于帮助网络安全专业人士理解和实施现有先进的网络安全技术与解决方案。无论读者是一名网络安全方面的专家，还是一名业内的新手，这本书都是一个宝贵资源。

许多关于网络安全方面的书籍，主要注重概念与理论。而本书却与之截然不同。本书可作为配置和管理 Cisco 市场领先动态链路的便捷工具书。这一链接存在于客户安全策略、用户或主机识别以及网络基础设施之间。本书的内容建立在 Cisco 安全解决方案中的关键要素之上。就如何成功地设置网络安全的各个方面提供实用的日常指导，涵盖诸如边界安全、安全识别、访问管理、数据隐私以及安全监控和管理等内容。

Yusuf Bhaiji 已在 Cisco Systems 工作了 7 年，现担任产品经理，负责 Cisco CCIE 安全验证拓展，同时他还是 Cisco Dubai 实验室的一名 CCIE 代理。Yusuf 对安全技术和解决方案的热情在他 17 年的行业经验和无数验证中表露无遗。作为安全技术领域的导师和顾问，Yusuf 丰富的阅历，磨炼了他将高技术含量的知识转化成一种简单直白，易于理解格式的能力。如果要寻求网络安全方面真正全面的向导，非 Yusuf Bhaiji 莫属！

Steve Gordon
Cisco Systems 副总裁
技术服务部
远程操作服务　Learning@Cisco

前　言

Internet 起源于 1969 年美国的 ARPANET 网络，是一个全世界松散连接的地区网络集合。单个计算机通过各种方式，如网关、路由器、拨号连接以及 Internet 服务提供商（ISP，Internet Service Providers）访问 Internet。如今，任何人都可以不受地域限制，通过 Internet 访问任何设备或计算机。

就像 Vinton G.Cerf 博士宣称的那样，“Internet 最不可思议的是，您可以连接到其他任何人。Internet 最糟糕的是，您可以连接到其他任何人。”

安然享受信息财富的同时也伴随着风险，因为有了 Internet，所有人的利害关系都有可能变得息息相关。风险包括从信息的丢失或损坏到信息的失窃，甚至更严重的信息事故。安全事件的数量正在急剧增长。

所有的这些情况极大地推动了网络安全的实施过程，以改善全世界所有组织机构的安全现状。如今，最复杂的网络需要最完善的安全解决方案。

在过去的几年中，安全已经逐步演变成为业内发展最迅速的领域之一。信息安全是所有组织机构的重要议程。公司需要保持信息安全，对能够解决问题的 IT 专业人员的需求在不断增加。

单点产品已不足以应对信息的保护和所需系统级的安全解决方案。在设计拥有主动和自适应安全系统以防御新出现的零天攻击的现代网络的过程中，链路端点和网络的安全显得尤为重要。

安全不再仅仅是一项使能技术或者权宜一时的事物，它已经成为网络蓝图的必要组成部分。安全技术和解决方案需要从根本上整合到基础设施中，与网络构架融合。今天的安全需要综合的端到端解决方案。

目标和方法

本书是一本综合参考书，涵盖所有主要的 Cisco 安全产品、技术和解决方案，是帮助网络专业人士理解和实施当前先进安全技术和解决方案的完整参考。本书涉及的范围广泛，深度足够为读者提供概念、设计和实施指导以及基本配置技巧。

通过一种易于理解的方式，这个无价资源将作为实施端到端安全工作的安全专业人士的安全中心知识库。

本书未对知识水平作任何假设，从而确保读者能看到一个有意义同时易于理解的解释。本书循序渐进，提供从每种技术的基本级别到每个主题的更详细的描述和讨论。

拥有这本权威参考用书，读者将对可用解决方案有一个较深入地理解，并学习如何在现今异构基础设施中构建综合安全网络。

本书涉及内容广泛，包括成熟及新近出现的技术信息，如自适应安全设备（ASA，Adaptive Security Appliance）防火墙软件 8.0 版本，Cisco 入侵防御系统（IPS，Intrusion Prevention System）感应软件 6.0 版本，主机 IPS，Cisco 群组加密传输 VPN（GETVPN，Group Encrypted Transport VPN），MPLS VPN 技术，Cisco 分布式拒绝服务（DDoS，Distributed Denial-of-Service）异常检测和缓解方案，Cisco 安全监控、分析和响应系统（CSMARS，Cisco Security Monitoring，Analysis，and Response System）以及安全构架、标准和法规遵从性，等等。

本书的读者

无论是对网络工程师或安全工程师、顾问，还是做安全认证方面研究的读者，本书都将成为设计和构建一个安全网络的重要参考。

此外，本书为拟参加 CCIE 安全认证考试的读者提供了涵盖新大纲考点的宝贵的备考资源。

本书可作为任何网络专业管理或考虑开发和实施 Cisco 网络安全解决方案与技术人员的参考书。

本书的内容结构

本书旨在补充可在 Cisco.com 和 Cisco 安全产品文件中获得的信息。本书共分为 5 个部分，把 Cisco 安全技术和解决方案归纳为 5 方面内容。

第 1 部分，“边界安全”：这一部分提供了控制访问关键网络应用、数据和服务的方法，以保证只有合法的用户和信息允许通过网络。第 1 部分包括以下章节：

- 第 1 章介绍网络安全原则、安全模型、安全标准的基本概述、策略以及网络安全框架。
- 第 2 章描述利用访问控制列表（ACL，Access Control Lists）执行流量过滤的能力。包括多种类型 ACL，如标准和扩展 ACL、锁与密钥、自反、时间、接收 ACL、基础设施 ACL 和传送 ACL。这一章依据 RFC 和最佳的通用实践讲述流量过滤。

- 第 3 章包括设备强化和路由器安全管理访问，防火墙设备和入侵防御系统（IPS，Intrusion Prevention System）设备最常用的技术。
- 第 4 章提供了全面交换机可用的综合安全特性设置。本章包括第 2 层端口级别安全控制、安全特性和交换机可用的最佳实践。
- 第 5 章介绍基于软件的 IOS 防火墙特性，包括陈旧的基于环境的访问控制（CBAC，Context-Based Access Control）和新引入的路由器上可用的区域式策略防火墙特性（ZFW，Zone-Based Policy Firewall）。
- 第 6 章涵盖基于 Cisco 防火墙产品硬件的全部范围，包括 Cisco PIX、Cisco ASA 防火墙设备以及 Cisco 防火墙服务模块（FWSM，Firewall Services Module）。本章完整说明了防火墙操作系统（OS，Operating Systems）软件特性和能力范围。
- 第 7 章是唯一一章详细地讲述常见攻击类型，并给出了各种攻击的表征和区分各种攻击的方法。本章提供了当第 2 层和第 3 层受到大范围攻击时所采用的防御技术。

第 2 部分，“身份安全和访问管理”：身份是对网络用户、主机、应用、服务和资源精确并主动的识别。第 2 部分包括以下章节：

- 第 8 章包括验证、授权和审计（AAA，Authentication，Authorization，and Accounting）体系和 AAA 技术的实施。本章包括访问管理时被执行的两个广泛应用的安全协议：RADIUS 和 TACACS+协议。
- 第 9 章给出 Cisco 安全访问控制服务器（ACS，Access Control Server）软件的详细情况，这一软件支持 AAA 技术和第 8 章讲到的安全协议。本章重点强调常用的 ACS 软件功能和特性。
- 第 10 章讲述使用多因素验证系统的识别和验证机制，介绍常见的双因素机制。
- 第 11 章包括建立在基于身份的网络服务（IBNS，Identity-Based Networking Services）技术基础上的授信与身份管理解决方案；提供了使用 IEEE 802.1x 技术，在第 2 层实施基于端口的验证和控制网络访问的详细介绍。
- 第 12 章概述了无线局域网（WLAN），进一步说明保障 WLAN 网络安全的细节。本章包括用于保护 WLAN 和扩展各种 EAP 协议的多种技术，包括 EAP-MD5、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP 和 Cisco LEAP 技术。本章还给出了常见 WLAN 攻击和防御技术的覆盖范围。
- 第 13 章详细讲述使用基于设备和基于架构的 Cisco 网络准入控制的 Cisco 自防御网络（SDN，Self-Defending Network）解决方案。本章包括实施 Cisco NAC 设备解决方案和 NAC-L3-IP、NAC-L2-IP 和 NAC-L2-802.1x 解决方案。

第 3 部分，“数据保密”：当必须保护信息免于被窃取时，能提供所需的验证、保密通信功能是极为重要的。在网络层使用安全服务对通信双方都有利。VPN 解决方案利用机密性、完整性和位于不可信任或公共网络，尤其是在 Internet 上任何地点的设备间的验证协议，保护通信的畅通。第 3 部分包括以下章节：

- 第 14 章是数据隐私和如何使用加密方法和加密解决方案保护通信的基础。这一章给出了各种加密算法的概述，包括散列算法、对称密钥和非对称密钥算法。
- 第 15 章是一个综合性章节，涵盖各种类型的 IPSec VPN 解决方案。本章给出各种 VPN 部署类型，重点放在 IPSec VPN 技术，包括 IPSec 协议、标准、IKE、ISAKMP

和 IPSec 的简介。本章还提供了使用多种方法实施 IPSec VPN 解决方案的完整范围。

- 第 16 章包括动态多点 VPN 解决方案体系结构，讲述设计、部件和 DMVPN 如何运行，还给出了实施各种类型 DMVPN 中心到节点和节点到节点的解决方案。
- 第 17 章包括使用创新的无需隧道的 VPN 方法保证数据安全性，讲述最新推出的 GET VPN 技术、解决方案的结构、组成部件以及 GET VPN 的运行方式。
- 第 18 章描述了基于 SSL 的 VPN 解决方案体系结构和各种类型的 SSL VPN。本章还涵盖最新引进的 Cisco 任意连接 VPN 技术。
- 第 19 章给出了基于多协议标签交换的 VPN 技术涵盖范围，通过 MPLS 网络提供数据安全性；介绍 MPLS VPN 解决方案体系结构和各种类型可用 MPLS VPN 技术。本章涵盖在第 2 层（L2VPN）和第 3 层（L3VPN）上基于 MPLS VPN 的实施解决方案。

第 4 部分，“安全监控”：为确保网络持续的安全，定期测试和监控安全准备状态十分重要。网络漏洞扫描可以主动发现薄弱的区域，当出现这种情况时，入侵检测系统可监控并响应安全事件。通过使用安全监控解决方案，组织机构可以获得对网络数据流和网络安全形式空前的可视性。第 4 部分包括以下章节：

- 第 20 章涵盖使用基于网络设备的传感器技术和入侵防御系统（IPS）的网络安全监控。本章全面介绍传感器操作系统（OS）软件功能和特性。
- 第 21 章涵盖使用基于主机的技术和主机入侵防御系统（HIPS，Host Intrusion Prevention System）的网络安全监控。本章详细叙述 Cisco 安全代理（CSA，Cisco Security Agent），并提供解决方案的体系结构、组成部分和使用 CSA MC 的 CSA 部署。
- 第 22 章详细描述使用 Cisco 异常检测和缓解系统的基于异常的安全监控所涉及的内容。本章包括 Cisco 流量异常检测器和 Cisco Guard 防护产品，用于提供 DDoS 防御。
- 第 23 章涵盖了基于安全威胁缓解（STM，Security Threat Mitigation）系统的创新的安全监控、分析和响应系统。本章给出 CS-MARS 的主要概念和部署准则。

第 5 部分，“安全管理”：随着网络规模和复杂度的增大，集中策略管理工具的需求也随之增长。具有基于浏览器界面，可以分析、解释、配置和监控安全策略状态的精准工具，增加了网络安全解决方案的可用性和有效性。第 5 部分包含以下章节：

- 第 24 章详细描述了 Cisco 安全管理解决方案所涉及范围，这一解决方案使用 Cisco 安全管理器（CSM，Cisco Security Manager）软件和各种设备管理 *x*DM 工具，包括 SDM、ASDM、PDM 和 IDM。
- 第 25 章提供了一个安全标准、策略、法规遵从和最佳实践架构的综述。本章包括两种广泛使用的安全架构：ISO/IEC 17799 和 COBIT。本章还涵盖了法规遵从和立法行为，如 GLBA 法案、HIPPA 法案以及 SOX 法案。

本书是综合参考书，也是集安全字典、百科全书和管理员准则于一体的全能工具书。

本书中使用的图标


PC
路由器
工作组路由器
集线器
文件服务器
多层交换机
带有防火墙的路由器
IOS防火墙
PIX防火墙
CS-MARS
访问服务器
安全交换机
无线接入点
IP电话
NAC应用
VPN连接器
光纤服务路由器
检测器
Web 集群
安全终端
Cisco ASA 5500
安全交换机
安全路由器
无线信号
串行线路
电路交换线路
以太网线路

命令语法约定

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

第1部分　边界安全