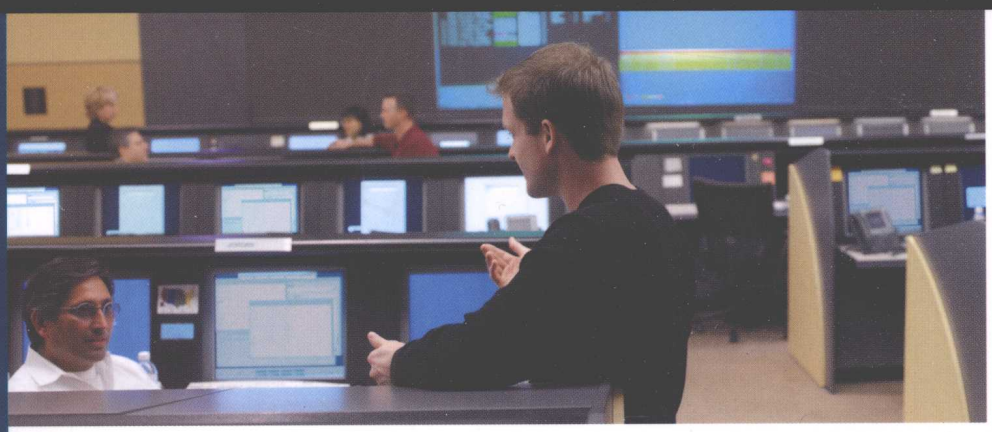
CCIE职业发展系列
CCIE Professional Development

ciscopress.com



网络安全技术与解决方案
（修订版）

Network Security Technologies and Solutions

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

〔美〕Yusuf Bhaiji，CCIE #9305 著
田果，CCIE #19036
刘丹宁，CCIE #19920 译

人民邮电出版社
POSTS & TELECOM PRESS

网络安全技术与解决方案
（修订版）

Network Security Technologies and Solutions

〔美〕Yusuf Bhaiji，CCIE #9305 著
田果，CCIE #19036
刘丹宁，CCIE #19920 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 ; 田果, 刘丹宁译. -- 2版（修订本）. -- 北京 : 人民邮电出版社, 2010.1
（CCIE职业发展系列）
ISBN 978-7-115-21734-9

Ⅰ. ①网… Ⅱ. ①海… ②田… ③刘… 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(2009)第202902号

版 权 声 明

CCIE 职业发展系列

网络安全技术与解决方案（修订版）

◆ 著 [美] Yusuf Bhaiji, CCIE #9305
译 田 果，CCIE#19036 刘丹宁，CCIE#19920
责任编辑 李 际
执行编辑 傅道坤

◆ 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
北京顺义振华印刷厂印刷

◆ 开本：787×1092 1/16
印张：38
字数：944 千字 2010 年 1 月第 2 版
印数：3 501－6 500 册 2010 年 1 月北京第 1 次印刷

著作权合同登记号 图字：01-2008-3326 号
ISBN 978-7-115-21734-9

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

本书包含了Cisco网络安全解决方案中最为常见的产品、技术，以及它们的配置方法和部署方针。

在产品方面，本书从硬件的PIX、ASA、FWSM模块、NAC设备、IDS、IPS、各类入侵检测模块、Cisco流量异常检测器、CS-MARS等，到软件的Cisco Secure ACS CSA、SDM和集成在各设备中的系统等，无所不包。

在技术方面，本书全面涵盖了Cisco网络中的各类安全技术，包括Cisco路由器、交换机上的多种攻击防御特性、CBAC、ZFW、各类WLAN安全技术、各类加密技术、VPN技术、IOS IPS技术等，无所不含。仅ACL技术一项，本书就分成了10余个种类并分别加以阐述。

在解决方案方面，本书以Cisco各类产品及其所支持的技术为纲，讲术了它们在不同环境、不同场合、不同媒介中的应用方法。

本书的任何一部分都始于理论，终于实践：开篇阐明某种攻击的技术要略，而后引入具体的应对设备、技术，以及部署和配置方法，作为相应的解决方案，纲举目张，博而不乱。

本书适用于网络工程师、网络安全工程师、网络管理维护人员，及其他网络安全技术相关领域的从业人员，可在他们设计、实施网络安全解决方案时作为技术指导和参考资料。尤其推荐那些正在备考安全方向CCIE的考生阅读本书，相信本书一定能够帮助他们更好地理解与考试相关的知识点，并为他们顺利通过考试铺平道路。

关于作者

Yusuf Bhaiji，CCIE #9305（路由交换和安全）在Cisco任职已达7年，现任Cisco CCIE安全认证的项目经理和Cisco迪拜Lab考场的考官，此前担任悉尼TAC安全与VPN小组的技术负责人。

早在Yusuf获得计算机科学硕士学位时，他对安全技术和解决方案就表现出了极高的热情，这种热情现已陪伴他度过了17年职业生涯。这可以通过他获得的大量认证得到充分体现。

Yusuf对于能够让别人分享他的知识而津津乐道，他本人也因此成为了众多新员工的良师益友，另外，他还在全球范围内设计并讲解了大量的网络安全解决方案。

Yusuf是多家非盈利性机构的咨询委员会成员，为此，他要出席各种学术活动与专业活动，来为这些机构宣传和推广一些互联网领域的技术以及这些技术的内在优势。Yusuf还在巴基斯坦网络工程师协议及IPv6论坛的巴基斯坦分部担任主席。

Yusuf曾撰写了一本名为《CCIE安全Lab实战》的著作，该书已于2004年初由Cisco出版社出版。他也担任了多本Cisco出版社出版物的技术审稿人，并撰写多篇文章、白皮书、报告，其中涉及多种安全技术。他经常兼任讲师，在各类世界性会议和专家讨论会中进行演讲，并因此赢得了较高的知名度。

关于技术审稿人

Nairi Adamian，CCIE 安全#10294，1999 年加盟 Cisco，现任 Cisco 澳大利亚的技术支持经理。她在 Cisco 技术支持中心（TAC）负责领导一支由客户支持工程师组成的团队。她拥有悉尼科技大学（UTS）计算科学专业的学士学位和麦觉理管理研究所（MGSM，Macquarie Graduate School of Management）的 MBA。

Kevin Hofstra，CCIE#14619，CCNP、CCDP、CCSP、CCVP，负责管理一个美国国防部空军通信代理机构的网络工程部门。Hofstra 先生拥有耶鲁大学计算机科学系的学士学位、科罗拉多大学的通信工程硕士学位和工程管理硕士学位。

Gert DeLact，CCIE#2657，是 Cisco CCIE 团队的产品经理。Gert 著有《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），他现在居住在比利时的布鲁塞尔。

献　词

谨以此书献给我的爱妻 Farah。在她的支持和鼓励下，这本书才最终得以问世。

致　谢

我要在此感谢我的家人，他们无时无刻不在给予我支持和鼓励。特别是我的父亲 Asghar Bhaiji，他的睿智总能使我获益良多。最后，在此对我的母亲 Khatija Bhaiji 表示怀念，她的爱始终可以我感受到阳光般的温暖。

我要感谢技术审阅 Nairi Adamian、Ger DeLaet 和 Kevin Hofstra，他们都为本书的出版作出了重大的贡献。在这本书问世之时，我谨对他们提出的宝贵反馈意见，及为书中每个主题所做的研究深表谢意。

由衷感谢 Brett Bartow 和开发团队的全体同仁，Betsey Henkels、Dayna Isley、Barbara Hacha、San Dee Phillips、Chris Cleveland，以及 Cisco Press 中参与这个项目的所有员工。他们专业的指导是这本书最终得以完成的关键因素。

我还要借此机会感谢我的经理，同时也是 Learning@cisco 团队的领导，Sarah DeMark，还有我在 Cisco 的同事们。无论是在我写作这本书时，还是在我完成其他项目时，他们都一如既往地给予了我支持，和他们共事让我获益良多，能够成为这个团队的成员是我的骄傲。

最后，还要感谢您——本书的读者朋友们——是你们的帮助成就了这本书。

序

在互联网经济蓬勃发展的大背景下，网络系统无疑承担着重大的时代使命，而网络系统必力求稳定，成为了这个时代的人心所向、大势所趋。无论是企业的客户、员工还是供应商，无不由衷期待企业领导和网络管理员有能力为他们打造一个绝对安全的网络环境，使他们能够随时获取网络中的资源，并能随时访问网络中的各类应用和数据。我们所面临的已经不再是单纯的挑战，还必须面对因网络安全一朝遭到破坏，而有可能给我们带来的巨大损失。

《网络安全技术与解决方案》这本书全面、翔实地阐述了管理 Cisco 网络的方法，在它的指导下，网络安全技术人员可以更好地理解和实施当前最高端的安全技术和解决方案。无论是对网络安全专家还是初学者，这本书都是实属难得的宝贵资源。

网络安全方面的书籍大都将重点放在了阐述概念和理论上，而《网络安全技术与解决方案》一书即打破了这种常规，它是一本着眼于配置和管理 Cisco 动态链路的实用型工具书。在占有市场主导地位的 Cisco 链路环境中，包含了客户的安全策略、用户或主机的身份以及网络设备。而这本书以 Cisco 安全解决方案的核心要素为纲，介绍了正确配置各类网络安全技术最为实际，应用也最为广泛的指导方法，这些技术涵盖了安全边界、身份安全与访问管理、数据保密，及安全监视和管理等方面，几乎无所不包。

Yusuf Bhaiji 已在 Cisco 任职 7 年，现为 Cisco CCIE 安全认证的项目经理和 Cisco 迪拜 Lab 考场的考官，此前担任悉尼 TAC 安全与 VPN 团队的技术负责人。早在 Yusuf 获得计算机科学硕士学位时，他对安全技术和解决方案就表现出了极高的热情，这种热情现已陪伴他度过了 17 年的职业生涯。他所获得的大量认证就是他钟爱此类技术的最好体现。Yusuf 在网络安全领域拥有丰富的执教阅历，

这种经验磨砺了他的表达能力，使他能够将高深的技术用简明扼要、通俗易懂的方式娓娓道来。如果您正打算购买一本涵盖广泛网络安全技术指导类书籍，这本书绝对不容错过。

Steve Gordon
Cisco Systems 公司
技术服务部副总裁
远程维护服务与学习@Cisco

前　言

Internet 诞生于 1969 年，它的前身 ARPANET，是由美国国防部高级研究计划署投资建立的。Internet 将零散地分布于世界各地的网络连接了起来，个人计算机用户可以用多种方式对它进行访问，比如通过网关、路由器、拨号连接和通 Internet 服务提供商等。现在，人人都可以通过 Internet 达到其中的任何一台设备/计算机，而不会受到地缘因素的制约。

这一切正如 Vinton G. Cert 博士所言："互联网的美妙在于它可以将你同任何人连接在一起，互联网的可怕在于它可以将你同任何人连接在一起。"

就在人们享受着能够自由获取信息的乐趣时，风险也随之而来，因为 Internet 上的任何人之间都有可能存在利益关系。这些风险从信息丢失到诽谤他人、盗用信息不一而足，安全事故的数量也得到了显著的增长。

在所有这一切纷至沓来的时候，世界各地的每一家机构都在期待他们的网络安全功能能够用更加强大的设备来实施，使安全性得到增强。在今天，越复杂的网络往往也就需要越全面且综合的安全解决方案。

在过去的几年间，安全的功能得到了提升，它成为了业内发展最快的领域之一，所有机构都将信息安全提上了议事日程。企业信息的安全性需要得到保障，能够帮助企业提高信息安全性的 IT 人才日益紧俏。

仅在某一点部署设备已经无法适应保护信息安全的需要，系统级安全解决方案成为了时代新宠。链接终端、网络安全，以及可以防御新型零时差攻击的主动防御和自适应安全系统成为了当今设计网络必须考虑的核心要素。

安全已经不再是网络中一项可有可无的技术了，安全问题也无法再像过去一样可以一劳永逸地得以解决；它已经成为了网络设计蓝图中不可忽视的组成部分。安全技术与解决方案必须从根本上集成进网络的设备中，融入到网络的结构里。今天的安全需要一个完整的端到端解决方案。

目标与方法

Cisco 网络安全技术与解决方案是一本涉及面广泛的参考书，它包含了所有主流 Cisco 的安全产品、技术和解决方案。这本参考大全可以帮助网络从业人员理解和实施当前高端的安全技术和解决方案。本书涵盖虽广，但是内容的深入程度足以帮助读者掌握其中涉及的概念、设计与实施的指导方针和基本配置技巧。

本书内容通俗易懂，它就像一座安全知识宝库，其中所蕴涵的无价资源可供安全从业人员随意取用，并帮助他们实施端到端的安全解决方案。

阅读本书并不需要较多的知识基础，可以确保读者有能力读懂其中的信息并同时消化吸收。它由各项技术的基础知识着手，循序渐进地为读者描述更加具体的信息，并带领读者探讨更加深入的内容。

有了这本可靠的参考资料，读者就能够掌握各种解决方案并学会如何搭建综合安全网络，并且这个网络还可以由不同厂商的设备构成。

这本书涉及面广，其中既有成熟的技术，也有刚刚出现的技术，如自适应安全设备（ASA，Adaptive Security Appliance）防火墙 8.0 版系统、Cisco 入侵防御系统（IPS，Intrusion Prevention System）传感器 6.0 版系统、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）异常检测与缓解方案、Cisco 安全监控、分析和响应系统（CSMARS，Cisco Security Monitoring，Analysis，and Response System）以及安全架构、标准和需要遵从的法规等。

本书的读者

不管您是一位网络工程师、安全工程师、顾问还是一名准备参加安全认证考试的学生，本书都会在您设计和搭建安全网络时成为您最主要的参考资料。

除此之外，对于准备参加 CCIE 安全认证考试的考生来说，本书也是非常宝贵的资源，因为它涵盖了新版课程计划中的全部主题。

本书可以作为所有网络从业人员在管理、研究、实施 Cisco 网络安全解决技术与方案时的参考。

本书的内容结构

本书是对 Cisco.com 和 Cisco 安全产品文档中已有信息所做的补充说明。

本书共分为 5 个部分，将 Cisco 安全技术解决方案划分为 5 个方面的内容。

第 1 部分，“边界安全”：这一部分介绍了如何控制去往重要网络应用、网络数据和网络服务的访问，以确保只有合法的用户和信息才能够通过网络。第 1 部分包括以下章节。

- 第 1 章“网络安全概述”介绍了网络安全原则、安全模型，并对安全标准、策略以及网络安全框架进行了基本概述。
- 第 2 章“访问控制”描述了如何利用访问控制列表（ACL，Access Control Lists）实现流量过滤功能。本章包括多种类型的 ACL，如标准和扩展 ACL、锁和密钥、自反、

时间、限速 ACL、设备保护 ACL 和过境 ACL。这一章依据 RFC 和最佳通用做法，讲述了如何过滤流量。

- 第 3 章“设备安全”包含了在加固设备中和保护路由器、防火墙设备及入侵防御系统（IPS，Intrusion Prevention System）设备管理访问中最常使用的方法。
- 第 4 章“交换机安全特性”介绍了交换机上的综合安全特性集。本章包括第 2 层端口级别的安全控制及交换机上的安全特性和最佳做法。
- 第 5 章“Cisco IOS 防火墙”介绍了基于软件的 IOS 防火墙特性，包括路由器上经典的基于环境的访问控制（CBAC，Context-Based Access Control）和新引入的基于区域的策略防火墙特性（ZFW，Zone-Based Policy Firewall）。
- 第 6 章“Cisco 防火墙：设备与模块”涵盖了所有 Cisco 硬件防火墙产品，包括 Cisco PIX、Cisco ASA 防火墙设备及 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）软件特性及其功能。
- 第 7 章“攻击向量与缓解技术”是相对独立的一章，这一章详细介绍了常见攻击类型及如何分类和识别各类攻击的方法。本章还为大量第 2 层和第 3 层攻击提供了相应的防御技术。

第 2 部分，“身份安全和访问管理”：身份用来准确而主动地识别网络中的用户、主机、应用、服务和资源。第 2 部分包括以下章节。

- 第 8 章“保护管理访问”包含了认证、授权和审计（AAA，Authentication，Authorization，and Accounting）体系的详细内容和 AAA 技术的实施方法。这一章还包括两种广泛应用于访问管理的安全协议：RADIUS 和 TACACS+协议。
- 第 9 章“Cisco Secure ACS 软件与设备”介绍了 Cisco Secure 访问控制服务器（ACS，Access Control Server）操作系统的详细情况，该系统支持 AAA 技术和第 8 章讲到的安全协议。本章还着重介绍了 ACS 操作系统中常用的功能和特性。
- 第 10 章“多重认证”讲述了使用多重认证系统的识别和认证机制，这一章介绍了常见的双重认证机制。
- 第 11 章“第 2 层访问控制”包含了建立在基于身份的网络服务（IBNS，Identity-Based Networking Services）技术基础之上的 Cisco 信任与识别管理解决方案；还详细介绍了使用 IEEE 802.1x 技术，在第 2 层实施基于端口的认证并控制网络访问的方法。
- 第 12 章“无线局域网（WLAN）安全”概述了无线局域网（WLAN）和保护 WLAN 的具体内容。这一章讲述了多种可以保护 WLAN 和扩展各类 EAP 协议的技术，包括 EAP-MD5、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP 和 Cisco LEAP 技术。本章还涵盖了常见 WLAN 攻击和缓解技术。
- 第 13 章“网络准入控制（NAC）”详细讲述了使用基于设备和基于架构的 Cisco NAC（网络准入控制）来实现的 Cisco 自防御网络（SDN，Self-Defending Network）解决方案。这一章包括了 Cisco NAC 设备解决方案及实施 NAC-L3-IP、NAC-L2-IP 和 NAC-L2-802.1x 解决方案的实施方法。

第 3 部分，“数据保密”：在信息必须通过保护而免于窃听危险的环境中，适时地提供认证、机密通信功能是极为重要的。在网络层使用安全服务能获得最有效的保护。VPN 解决方案在位于不可信或公共网络中（特别是 Internet）的通信双方之间通过机密性、完整性和认证协议确保通信的安全。第 3 部分包括以下章节。

- 第 14 章“密码学”是数据隐私以及使用加密方法和密码学解决方案确保通信安全的基础。本章概述了各种加密算法，包括散列算法、对称密钥和非对称密钥算法。
- 第 15 章“IPsec VPN”涵盖了全面的 IPSec VPN 解决方案。本章给出各种 VPN 部署类型，重点讲述 IPSec VPN 技术，包括 IPSec 协议、标准、IKE、ISAKMP 和 IPSec profile。本章还列举了使用多种方法实施各种类型的 IPSec VPN 解决方案。
- 第 16 章“动态多点 VPN（DMVPN）”介绍了动态多点 VPN 解决方案技术架构，描述其设计、组件和 DMVPN 的工作方式，还给出了各种类型 DMVPN 解决方案的实施案例，包括中心到节点和节点到节点解决方案。
- 第 17 章“群组加密传输 VPN（GET VPN）”涵盖了使用创新的无需隧道 VPN 方法确保数据的安全，详细介绍了最新引入的 GET VPN 技术、解决方案技术架构、组件以及 GET VPN 的工作方式。
- 第 18 章“安全套接字层 VPN（SSL VPN）”介绍了基于 SSL 的 VPN，涵盖 SSL VPN 解决方案技术架构和各种类型的 SSL VPN。本章同时介绍了最新引入的 Cisco AnyConnect VPN。
- 第 19 章“多协议标签交换 VPN（MPLS VPN）”介绍了使用基于多协议标签交换（MPLS）的 VPN 技术为穿越 MPLS 网络的数据提供安全保护，涵盖 MPLS VPN 解决方案技术架构以及各种可用的 MPLS VPN 技术。本章涵盖基于第二层（L2VPN）和第三层（L3VPN）的 MPLS VPN 解决方案的实施。

第 4 部分，“安全监控”：为持续确保网络安全，定期测试和监控安全准备工作的状态是十分重要的。网络漏洞扫描可以主动发现薄弱的区域，入侵检测系统可以监控并在发生安全事件时做出响应。通过使用安全监控解决方案，组织机构可以完全掌控网络数据流和网络安全状态，获得空前的可见性。第 4 部分包括以下章节。

- 第 20 章“网络入侵防御”涵盖使用基于网络的设备传感器技术——入侵防御系统（IPS）——进行网络安全监控。本章全面介绍了传感器操作系统（OS）软件的功能和特性。
- 第 21 章“主机入侵防御”涵盖使用基于主机的技术——主机入侵防御系统（HIPS）——进行网络安全监控。本章详细讲解 Cisco 安全代理（CSA）技术，包括其解决方案技术架构、组件和使用 CSA MC 的 CSA 部署。
- 第 22 章“异常检测与缓解”涵盖使用 Cisco 异常检测和防御系统进行基于异常的安全监控。本章介绍了 Cisco 流量异常检测器和 Cisco Guard 产品，用于提供 DDoS 防御。
- 第 23 章“安全监控和关联”涵盖了基于安全威胁防御（STM）系统的创新型安全监控、分析和响应系统（CS-MARS）。本章介绍了 CS-MARS 的核心概念和部署准则。

第 5 部分，“安全管理”：随着网络规模的扩大和复杂度的增加，对于集中式策略管理工具的需求也随之增长。提供基于浏览器的用户界面，可以分析、解释、配置和监控安全策略状态的先进工具，增强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“安全和策略管理”全面介绍了 Cisco 安全管理解决方案，使用 Cisco 安全管理器（CSM）软件以及各种设备管理 xDM 工具，包括 SDM、ASDM、PDM 和 IDM。
- 第 25 章“安全框架与法规遵从性”概述了安全标准、策略和法规遵从、最佳做法框架。本章包括两种广泛使用的安全框架：ISO/IEC 17799 和 COBIT。本章还涵盖了法规遵从和规章制度，其中包括 GLBA、HIPPA、SOX 法案。

本书是全面的参考书，是集安全字典、百科全书和管理员指南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 集中器
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，粗体字表示由用户手动输入的命令（如**show**命令）。
- *斜体字*表示用户应提供具体值的参数。
- 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