<<网络安全技术与解决方案>>

图书基本信息

书名：<<网络安全技术与解决方案>>

13位ISBN编号：9787115193117

10位ISBN编号：7115193118

出版时间：2009-3

出版时间：人民邮电出版社

作者：海吉

页数：565

字数：914000

前言

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。
YusufBhaiii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！

<<网络安全技术与解决方案>>

内容概要

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。

作者简介

作者：(美国)海吉 (Yusuf bhaiji) 译者：罗进文 王喆 张媛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Intemet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。

<<网络安全技术与解决方案>>

书籍目录

第1部分 边界安全 第1章 网络安全概述 1.1 网络安全的基本问题 1.2 安全范例的变化 1.3 安全准则——CIA模型 1.4 策略、标准、规程、基线、准则 1.5 安全模型 1.6 边界安全 1.7 各层的安全 1.8 安全轮 1.9 小结 第2章 访问控制 2.1 利用ACL的流量过滤 2.2 IP地址概述 2.3 子网掩码与反掩码概述 2.4 ACL配置 2.5 理解ACL的处理 2.6 访问列表类型 2.7 小结 2.8 参考 第3章 设备安全 3.1 设备安全策略 3.2 增强设备安全 3.3 安全设备的安全管理访问 3.4 设备安全清单 3.5 小结 3.6 参考 第4章 交换机的安全特性 4.1 保护第2层 4.3 专用VLAN（PVLAN） 4.4 交换机的访问列表 4.5 生成树协议的特性 4.6 监测DHCP 4.7 IP源保护 4.8 动态ARP检测（DAI） 4.9 Catalyst高端交换机的高级集成安全特性 4.10 控制层管制（CoPP）特性 4.11 CPU速率限制器 4.12 第2层安全的最佳实践 4.13 小结 4.14 参考 第5章 Cisco IOS防火墙 第6章 Cisco防火墙：设备和模块 第7章 攻击向量和缓解技术第2部分 身份安全和访问管理 第8章 安全访问管理 第9章 Cisco安全ACS软件和设备 第10章 多因素验证 第11章 第2层访问控制 第12章 无线局域网（WLAN）的安全 第13章 网络准入控制（NAC）第3部分 数据保密 第14章 密码学 第15章 IPSec VPN 第16章 动态多点VPN 第17章 群组加密传输VPN 第18章 安全套接字层VPN（SSL VPN） 第19章 多协议标签交换VPN（MPLS VPN）第4部分 安全监控 第20章 网络入侵防御 第21章 主机入侵保护 第22章 异常检测和缓解 第23章 安全监控和相关性第5部分 安全管理 第24章 安全和策略管理 第25章 安全框架和规章制度

章节摘录

插图：9.如何减小风险？
10.风险的承受能力有多大？
可以根据这些疑问讨论并回答一些与建立安全网络基本需求相关的基本问题。
网络安全技术能降低风险，为扩展企业内部网、外部网及电子商贸应用业务提供基础。
解决方案也能避免敏感数据和企业资源受到入侵和破坏。
现在，先进的技术能为中小型公司（SMB，small and medium-sized businesses）以及大型网络提供发展和竞争的机会；同时，这些技术还强调了保护计算机系统免受大规模安全威胁的必要性。
对于业务来说，保持网络基础设施安全的挑战已经变得前所未有的关键和重要。
尽管信息安全方面的投资相当大，但组织机构仍然被网上事件所困扰。
同时，管理部门追求使用较少的资源，以取得较大的成效。
因此，提高安全的有效性仍然很重要，如果没有必要，则加强可用性和灵活性也将成为首要目标。
如果没有适当的保护，网络的每个部分都容易经受到来自入侵者、竞争对手甚至是雇员的安全破坏行为或未经授权的破坏活动。
许多自己管理内部网络安全且上网不仅仅是进行邮件收发的组织机构会受到网络攻击——而大多数公司甚至都不知道自己遭受攻击。
较小的公司往往会怡然自得，产生安全错觉，经常只回应最近遭遇的病毒或最近公司网站的受损，但这些企业会陷入一种困境，没有足够的时间和资源用于安全防范。
为了解决这些问题，Cisco已开发出一套综合安全规划，建议和阐述了针对网络不同部位的特定安全方案。

媒体关注与评论

“ Yusuf是安全技术领域的导师和顾问，他丰富的阅历磨练了他将高技术含量的知识转化成一种简单直白、易于理解的形式的能力。
如果要寻求网络安全方面真正全面的参考书，则非本书莫属！
” ——steve Gordon，Cisco技术服务部副总裁

编辑推荐

《网络安全技术与解决方案》介绍了先进的网络安全产品和可行方案，能够帮助读者理解和实施最新的网络安全技术，以保障整个网络基础设施的通信安全。
在交换机上使用访问列表过滤流量。
实施安全功能；配置Cisco lOS路由器防火墙功能．部署ASA和PIX防火墙设备；理解攻击向量并应用2层和3层缓解技术；AAA安全访问管理；利用多因素验证技术的安全访问控制：实施基于身份的网络访问控制：应用最新的无线局域网安全解决方案；遵循Cisco NAC来执行安全策略；学习密码学基础并实施lPSecVPN、DMVPN、GET VPN、SSL．VPN和MPt-S VPN技术：使用网络和主机入侵防御、异常检测和安全监控及相关技术，监控网络活动和安全事件响应；部署Cisco安全管理器、SDM、ADSM、PDM和IDM等安全管理解决方案：学习GLBA、HIPPA和SOx等法规遵从性问题。
《网络安全技术与解决方案》是一个网络安全知识库。
涵盖了CIsco网络安全的各个方面，通过简单易懂的方式帮助读者实施端到端安全解决方案。
书中将CIsco安全技术和解决方案归纳为边界安全、身份安全与访问管理、数据保密、安全监控和安全管理5个部分。
这5个部分共同作用使得客户安全策略、用户或主机身份和网络基础设施之间的动态链接成为可能。
凭借这本权威的参考书。
读者能够更加深刻地理解可行的解决方案，并能学习到如何在现代异构网络体系中构建多业务安全网络。
对于那些寻求有关成熟或新兴安全策略的综合参考书的读者来说，《网络安全技术与解决方案》无疑是绝佳的首选。
《网络安全技术与解决方案》也是CClE安全考试极佳的学习指南。

版权说明