SECURITY

Cisco防火墙

Cisco Firewalls

Concepts, design and deployment for
Cisco Stateful Firewall solutions

〔巴西〕**Alexandre M.S.P. Moraes**，CCIE #6063 著
YESLAB工作室 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco防火墙

Cisco Firewalls

〔巴西〕**Alexandre M.S.P. Moraes**，CCIE #6063　著
YESLAB工作室　译

人民邮电出版社
北京

图书在版编目（CIP）数据

Cisco防火墙 / （巴西）摩赖斯（Moraes, A. M. S. P.）著 ; YESLAB工作室译. -- 北京 : 人民邮电出版社, 2014.8
ISBN 978-7-115-35172-2

Ⅰ. ①C… Ⅱ. ①摩… ②Y… 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(2014)第112727号

版 权 声 明

◆ 著 [巴西] Alexandre M.S.P.Moraes
译 YESLAB 工作室
责任编辑 傅道坤
责任印制 彭志环 杨林杰

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
邮编 100164 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：54.5
字数：1127 千字 2014 年 8 月第 1 版
印数：1–3 000 册 2014 年 8 月北京第 1 次印刷

著作权合同登记号 图字：01-2011-4675 号

定价：128.00 元

读者服务热线：(010)81055410 印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

本书采用理论结合配置案例的方式，对 Cisco 主流的防火墙产品、功能特性和解决方案进行了全面而详细的讲解，同时还介绍了如何将这些内容应用到网络安全设计和运维中。

本书共分为 17 章，主要内容包括防火墙和网络安全概述、Cisco 防火墙系列产品概述、防火墙配置基础知识、对防火墙进行排错所使用的工具、网络拓扑中的防火墙、虚拟化、如何让流量在部署或未部署 NAT 的环境中穿越 ASA、经典 IOS 防火墙概述、IOS 区域策略防火墙概述、其他防护机制、应用监控、语音协议检测、防火墙上的身份认证、防火墙与 IP 组播、防火墙与 IPv6，以及防火墙的互动等。

对设计和实施防火墙的网络工程师、网络架构师来讲，本书是一本必不可少的参考资料；同时，对于安全管理员、运维人员以及技术支持人士，本书也是一本难得的实用工具书；正在备考 CCNA 安全、CCNP 安全以及 CCIE 安全的考生，也可以从中获益。

序

当今网络在规模和复杂程度上，已经经历了爆炸式的成长，它已经成为了一项包罗万象的技术，实现网络安全的难度亦随之增加。核心网络的设计蓝图需要以强大的物理设备作为基础，而这可以通过在系统的核心部分集成防火墙设施来实现。现今，防火墙已经成为网络中的核心设备，成为每个网络环境中不可或缺的组成部分。

Alexandre M. S. P. Moraes 的这本大作旨在补充一些常常为人们所忽视的基本概念，他通过本书为读者提供了一个 Cisco 全系列防火墙产品的资源宝库。

Alexandre 使用了一种独特的方式来诠释防火墙技术的概念与结构。他独特的叙述方式彰显了他写作方面的功底，他能够用一种易于理解的方式一步一步地引导读者去理解这些当前常用的理论。他将当前常用的工具，与许多命令的输出信息结合起来，以便读者能够轻松理解各项技术，借此阐释它们的工作方式。

本书和其他同类主题的图书不同，本书不能被归类为一本配置指南或命令语法大全。它旨在向读者提供一些重要工具和一些核心技术，让读者能够掌握各类 Cisco 防火墙系列的产品。无论您是一位想要学习 Cisco 防火墙技术的初学者，还是一位正在寻找一本防火墙参考图书的资深工程师，您都能从这本书中找到自己期待的内容。

在如何设计、实施和维护高度安全的网络这一方面，本书是一本不可获缺的参考读物。这是一本必读之作，也是图书收藏中的必收之作——总之，这是一本难得一见的佳作。

——Yusuf Bhaiji

资深经理，专家认证持有者（CCIE、CCDE、CCAr）

关于 YESLAB 工作室

作为执国内高端 IT 培训之牛耳的企业，YESLAB 多年来深感本土图书数量的缺位、引进作品质量的参差。

有鉴于知识分享始终是 YESLAB 不变的追求，YESLAB 甘愿在培训市场之外，通过书作向华语同仁公开自己对 IT 的解读，以鼎精英之智，以传技术之功，以飨万千读者。

YESLAB 工作室应运而生，这是北京鼎智传承科技有限公司服务于技术读者的机构，旨在与人民邮电出版社就 IT 技术类专业图书的翻译和创作工作展开深入合作，践行“鼎智传承”之宗旨。

YESLAB 工作室的译作均由拥有大量译作的业内专家执笔，同时由 YESLAB 高级讲师和学员共同参与和审稿，尽一切可能为读者带来原汁原味的技术阅读体验。

YESLAB 工作室创作的本土化图书，全部是老余、现任明教教主、阿彭等技术精英；孙晨、戴鑫、闫斌等后起之秀的心血结晶，经由专长于写作的业内人士执笔润色，旨在让读者通过阅读，在事业上百尺竿头更进一步。

除了与人民邮电出版社深入合作之外，YESLAB 工作室还会与国内高校合作，陆续推出以校企合作为目标而定制的供高校师生使用的国家高校教材。

YESLAB 工作室期待能够在未来不断与各类高校和企业开展合作，一道创作更多佳品，为华语技术图书贡献力量。我们更加期待着能够参与本土华语技术图书的对外输出工作，让华人在全球技术领域发出自己的声音。

关于作者

Alexandre Matos da Silva Pires de Moraes，CCIE #6063，自 1998 年便开始在 Cisco（巴西）担任系统工程师，他参与的项目不仅涉及网络安全技术与 VPN 技术，同时也包含路由协议、园区网设计、IP 组播路由和 MPLS 网络设计。他曾经为大型企业和公共部门提供过技术支持，也曾在将近 3 年的时间里供职于巴西的一个安全工程师小组。Alexandre 拥有 CISSP、CCSP 和 3 项 CCIE 认证（路由交换、安全与服务提供商）。

Alexandre 是 Cisco Live 的一名活跃的讲师，他毕业于巴西航空理工学院（ITA）电子工程系，对数学有着难以抑制的热忱（尤其喜欢综合几何和三角函数）。

Alexandre 有一个私人博客，他会在这个博客上讨论与网络和安全技术有关的内容：http://alexandremspmoraes.wordpress.com/。

关于技术审稿人

Maurilio de Paula Gorito，CCIE #3807，是一名三料 CCIE，拥有路由交换、WAN 交换和安全三个方向的认证。Maurilio 在网络领域的工作经验超过 24 年，包括 Cisco 网络和 IBM/SNA 环境。Maurilio 的经验包括对运行 RIP、IGRP、EIGRP、BGP、OSPF、QoS 和 SNA 的大型 IP 网络进行规划、设计、实施和排错，并曾于美国和巴西任职。他在学校和企业讲授技术课程的经验达 10 年以上。他曾在 Cisco 担任 CCIE 实验考试的考官，及 CCIE 实验考试的项目经理。他曾在（美国加利福尼亚州）圣何塞的 CCIE 实验考试中心监考过 CCIE 路由交换和 CCIE 安全实验考试。作为这个项目的项目经理，Maurilio 负责管理 CCIE 路由交换考试实验部分和笔试部分的题目开发工作。Maurilio 也曾在 Cisco 研讨会上发表过重要的讲演。目前，Maurilio 在 Riverbed Technology 担任认证经理，负责管理 Riverbed 的认证项目。他拥有数学和教育学领域的学历。

Allan Eduardo SáCesarini，CCIE #5440，是一位双料 CCIE，分别于 1999 年和 2001 年获得了路由交换和服务提供商方向的认证。他在 Cisco 任职达 12 年以上，曾为银行、公共事业部门、政府机构、面向企业客户的服务提供商、宽带服务商等机构提供过技术支持，近期曾为有限电视运营商提供过支持。Allan 曾经使用过的技术数不胜数，包括 SNA/IBM、IPX、（规模大小不等的）IP 路由、园区 LAN 与 ATM 网络、IP 电话通讯与语音会议解决方案、基于 Docsis（有线数据传输服务接口规范）的数据服务及数字电视。Allan 当前在 Cisco 高级服务部（Csco Advanced Service）担任顾问，并且在 Cisco 研讨会和 Cisco Live 中以 LAN 体系结构、MPLS 技术和安全解决方案等为主题发表过演讲。

Allan 拥有巴西航空理工学院（ITA）颁发的计算机工程学位，当前他正在 FGV（Fundacão Getúlio Vargas）攻读 MBA 企业管理学位。

献辞

本书献给我的爱妻 Rachel，与我可爱的孩子 Eduardo 和 Gustavo，他们都是我灵感的真正来源。除了他们给与我的耐心与支持之外，我永远也不会忘记在写作之时与他们的对话：

Eduardo（当时 6 岁）问我：

“爸爸，这本书比你儿子还重要吗？”

“爸爸，我们再也不会一起下棋和踢球了吗？”

“爸爸，别忘了跟你的书道晚安。”

Gustavo（当时 3 岁，他对 Cisco Press 出版物封面的颜色更感兴趣）

“爸爸，这本书为什么不是紫色的？”

“爸爸，你什么时候能写本绿的？”

本书同样献给我的母亲 Lélia，她用言传身教的方式告诉了我如何实现目标，永不放弃。

最后，我愿将本书献给我的 3 位恩师，他们真正影响了我的人生，成就了我的发展，他们是：Seizi Amano，我心目中永远的数学宗师，对于我的努力不断给与支持；还有你，我的朋友，José AcácioViana Santos，我怎么会忘记你呢？你教给了我写作是锤炼思考的一种方式，你使我相信，写作只是问题的解决方法而非问题本身；还有 Roberto Stanganelli，无论距离与环境，你总是无处不在地向我传递着乐观的生活态度。

致谢

我想在此向我的 3 位特殊的朋友表达我的谢意，他们与我分享了他们对本书内容与形式的想法，正是他们让本书对读者更有助益，他们是 FredericoVasconcelos、Gustavo Santana 和 Diego Soares。

感谢我的好兄弟 Andre Lee，感谢你提供的艺术插图，这是多棒的一份厚礼啊！

还要感谢 Marcos Yamamoto、Renier Souza 和 Renato Pazotto，感谢他们在我参与项目的早期为我提供的帮助。

感谢本书的技术审稿人 Allan Cesarini 和 MaurilioGorito，正是他们作出的巨大努力才让本书变得更加准确。

我要感谢 IOS 安全团队中一些朋友，他们帮助我创作了 AAA 或 ZFW 中的部分内容，他们是 Nelson Chao、Arshad Saeed、SrinivasKuruganti、Umanath S. S 和 PrashanthPatil。

感谢帮助我完成了本书第 13 章的语音团队成员：Christina Hattingh、Pashmeen Mistry、Dan Keller 和 Praveen Konda。

感谢在审校环节中，为本书提供了帮助的 Andrew Cupp 和 Ginny Munroe，谢谢你们付出的耐心。

感谢 Pearson 团队的所有成员，他们将这份作品的最终版本转化为实物。

特别要感谢 Brett Bartow，你能理解市面上仍有（提供各类技术方法的）防火墙类图书的市场空间，并能对这个项目实实在在地投入，对此我铭感五内。

前言

在保护网络这一方面，防火墙一贯被视为一种重要的组成部分。虽然防火墙技术并不是一个新鲜的话题，但在设计安全网络时，许多极有帮助的重要概念和资源却常常被人们忽视，甚至忽略。

这本书旨在介绍 Cisco 防火墙的各类功能与产品，以及如何通过结构化的方式对这些功能和产品进行分类，以建立安全解决方案。

这本书的创作动机与一个朴素的真理有关：对各个特性的理解越深入，就越能将他们应用在设计当中。毕竟，创建更安全的设计方案，是每一个真心希望投身于网络安全领域的人，最终的目的。

“幸福就是将所知所学转化到教学之中。”

——CoraCoralina，巴西诗人

目标和方法

典型的防火墙图书分为两类。

- 配置指南和配置手册，重在介绍实施某些特性的命令集。这类图书确有其重要性，但它们往往忽略了这些特性的作用，以及使用该特性的理由进行介绍，因此对于帮助读者构建使用这些特性的知识体系收效甚微。
- 还有一类纯理论教材，仅通过一种笼统的方式对各类防火墙进行介绍，而不会专门介绍“如何在某个平台上实现某些功能”，也往往不会将理论联系实际。

将理论联系实际可以帮助读者理解很多重要的概念，而且可以帮助读者设计出更好的网络方案。拥有理工背景的人都明白这个道理：下功夫研习理论，理解如何使用这些基础理论，对于解决实际问题十分必要。

这里还有一点必须说明，即在很多同类图书中，排错方法往往会被列入图书的附录之中，与正文所在之处完全脱节。但本书采用了一种截然不同的方式：我们将各类用以排错的工具都应用到了本书中，以展示防火墙特性的工作方式。正是通过这种方法，本书才得以将理论联系实际。在熟悉了这些排错工具之后，希望读者能够不断回顾这些工具，以加强对各章中理论知识的理解。这不仅可以帮助读者学习这些知识，也可以在实际部署环境中，协助读者解决一些排错中遇到的问题。

读者对象

本书旨在介绍 Cisco 产品中的防火墙功能，同时还从防火墙设备的角度介绍了设计安全网络的方法。无论是对于初学者还是经验丰富的工程师，都能在本书中找到关于 Cisco 防火墙的实用知识。本书的目标读者包括：

- 负责设计和实施防火墙解决方案的网络安全工程师与架构师；
- 那些希望深入理解（其部署的）防火墙功能的安全管理员和安全产品操作员；
- 需要对 Cisco 网络防火墙提供支持的专业服务工程师与 TAC 工程师；
- 正在学习 Cisco 安全课程（如 CCNA 安全、CCNP 安全和安全 CCIE 实验）并准备考取认证的学员。

虽然本书中包含了很多与配置有关的内容，但这绝非是一本配置指南。本书的创作初衷是让读者深入理解防火墙的各项功能，以及防火墙特性的最佳做法（无论是在安全设计方案中独立使用，还是与其他特性进行集成）。

本书组织结构

本书既可以从头到尾通篇阅读，也可以根据需要进行跳读。本书中有一些以 ASA 为核心的篇章，也有一些专门针对 IOS 的章节，但大多数篇幅都会同时对这两种系统的配置进行介绍。这样做是为了更好地比较各个系统的用法，读者可以根据自己的需要选择最适合的实施方案。另一个优势在于，通过这种做法，每个理论概念都只需要介绍一次（而不需要在每个平台用到该理论时，都重复对其进行介绍）。

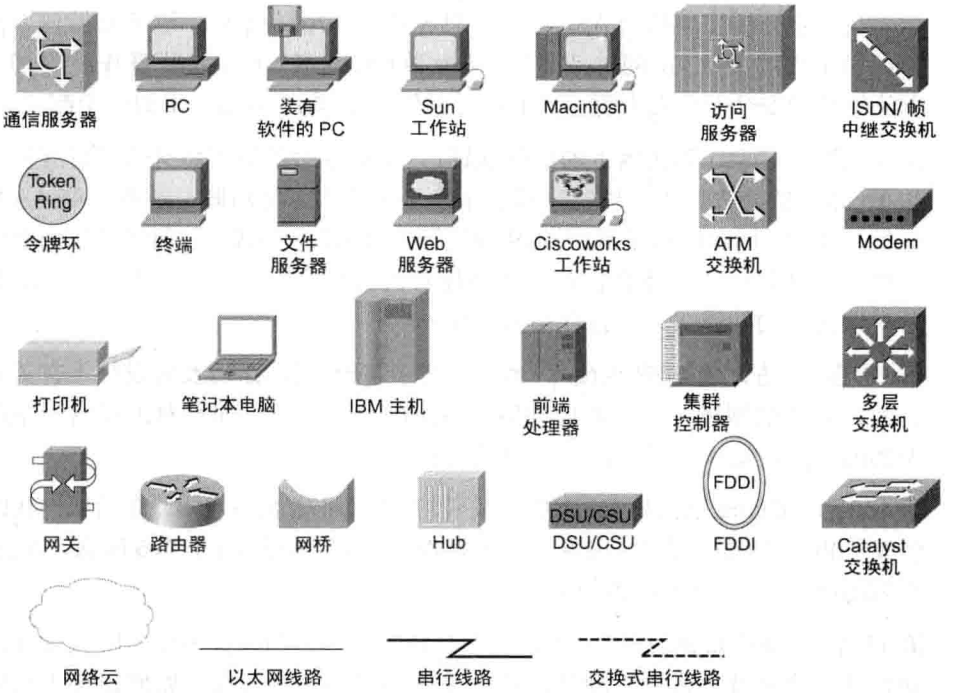
- **第 1 章，“防火墙与网络安全”**。在对安全策略的重要性进行了概述之后，本章对各类经典网络防火墙，以及将它们部署进网络环境中的方法进行了介绍。接下来，本章开始着重对状态化防火墙进行介绍，同时还介绍了它们是如何满足复杂网络环境中，各类技术需求的。
- **第 2 章，“Cisco 防火墙系列概述”**。本章旨在对可以使用状态化防火墙解决方案的各类 Cisco 硬件平台进行概述。本章也介绍了选择防火墙解决方案时，需要考虑的一些重要参数。
- **第 3 章，“防火墙配置基础”**。本章介绍了 Cisco 系列防火墙的初始配置工作，介绍的内容涵盖命令行配置界面（CLI）、启动进程、IP 地址选择、远程管理方法等。如果读者已经对 Cisco 设备比较熟悉，则可以跳过本章中的内容。

- **第 4 章，“工欲善其事，必先利其器”**。本章是本书的基础，因此，即使是资深工程师，也应通读这一章。本章中介绍的工具会在全书中反复使用，以介绍 Cisco 防火墙的工作方式，并将理论联系实际。
- **第 5 章，“网络拓扑中的防火墙”**。在介绍各类安全服务的作用之前，管理员需要通过 3 层或 2 层连接模型将防火墙部署进网络拓扑当中。本章的内容涵盖了桥接、静态路由、以及各类动态路由协议（如 OSPF、EIGRP 和 RIP）的相关内容。本章对于那些不是十分熟悉路由和桥接解决方案的安全从业者而言，具有重要的参考价值。
- **第 6 章，“防火墙世界中的虚拟化”**。本章介绍了网络环境中虚拟化的概念，同时介绍了如何将一些资源分割技术（如 VLAN、VRF、虚拟防火墙等）结合起来，建立一个强大而又安全的虚拟化体系。
- **第 7 章，“在没有部署 NAT 的环境中穿越 ASA”**。ASA 是本章的核心设备，本章也是首个真正开始介绍安全特性的篇章。本章的内容包括安全级别、连接的建立与断开、ACL 的处理以及对象组等重要概念，并分别通过案例对这些概念进行了讨论。
- **第 8 章，“在部署了 NAT 的环境中穿越 ASA”**。本章是对第 7 章的补充，本章会对网络地址转换（NAT）的概念进行详细阐述，同时还会介绍 ASA 防火墙可以使用的各类 NAT 技术。人们常常会产生疑惑的 NAT 优先级问题也将在本章中进行详细的研讨。附录 A 是对第 7 章和第 8 章内容的补充。
- **第 9 章，“经典 IOS 防火墙概述”**。本章涵盖了 IOS 系统中的 CBAC（基于上下文的访问控制）特性集，这一概念在这里会被称作经典 IOS 防火墙。本章中还介绍了其他一些重要的主题，如 NAT、ACL 和对象组，同时通过基于 IOS 的设备对这些特性进行了举例介绍。
- **第 10 章，“IOS 区域策略防火墙概述”**。本章介绍了区域策略防火墙（ZFW），此为 Cisco IOS 防火墙部署方案的第一选择。这一章还对建立 ZFW 策略的各个模块，以及可以对 4 层进行监控的安全功能进行了讲解。
- **第 11 章，“其他防护机制”**。本章的重点在于 4 层的保护资源，以及可以为状态化监控功能增值的保护技术。本章中涵盖的特性包括防欺骗、TCP 正常化、连接限制、IP 分片处理等。
- **第 12 章，“应用监控”**。本章介绍了各类 Cisco 系列网络防火墙的应用层监控功能。对于那些在穿越无状态数据包过滤特性时，或穿越只能工作在 4 层的状态化防火墙时，常常会遇到问题的应用协议，Cisco 防火墙中的这类功能便可以发挥作用。

这种具备应用层知识的特性也可以应用在某些更加复杂的过滤行为中。

- **第 13 章，“语言协议的监控”**。本章根据第 12 章中介绍的应用监控知识，详细分析了如何对经典的 IP 电话通讯协议（如 SCCP、H.323、SIP 和 MGCP）进行监控。本章还进一步分析了高级的 ASA 功能（TLS 代理和电话代理），这些功能可以提供语音的机密性解决方案，同时又不失状态化监控的优势。对于那些对 IP 电话通讯技术并不熟悉的安全专业人士而言，本章可以作为了解 IP 电话技术的一个起点。
- **第 14 章，“Cisco 防火墙上的身份认证”**。本章分析了如何将身份信息应用于所有 Cisco 系列的防火墙上，以实现基于用户身份的状态化功能。本章也对 AAA 架构进行了探讨，同时比较了 RADIUS 协议和 TACACS+协议，并阐述了这两个协议各自适用的任务：前者适合控制那些穿越防火墙的访问，而后者则适合控制那些以防火墙为目的的连接（即管理访问控制）。
- **第 15 章，“防火墙与 IP 组播”**。本章介绍了与 IP 组播路由及转发技术有关的各个方面，并详细阐述了防火墙处理组播流量的方式。对于那些对组播这一主题并不熟悉的人员，这一章可以作为一个重要的参考。
- **第 16 章，“Cisco 防火墙与 IPv6”**。随着 IPv4 地址资源的耗竭，介绍下一代因特网协议（IPv6）就变得非常有必要了。本章也介绍了一些重要的 IPv6 概念，以及 Cisco 系列防火墙关于 IPv6 的各类安全特性。
- **第 17 章，“防火墙的互动”**。本章重在介绍安全网络的设计方法。防火墙功能与其他特性（或系统）进行互动可以提升总体的网络安全水准。如何定义“互动”常常与在一些特殊环境中部署防火墙时，所面临的挑战有关。
- **附录 A，“ASA 8.3 在 NAT 和 ACL 方面的变化”**。本附录旨在强调 ASA 8.3 版本中 NAT 模型的变化，因此读者不妨将附录中的内容与本书的第 8 章进行比较。定义全局 ACL（Global ACL）的方法也在这个附录中进行了介绍。

本书使用的图标



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