SECURITY

Cisco 安全防火墙服务模块 (FWSM) 解决方案

Cisco Secure Firewall Services Module (FWSM)

Best practices for securing

〔美〕 Ray Blair，CCIE #7050
Arvind Durai，CCIE #7016 著

孙余强　李雪峰　译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 安全防火墙服务模块 (FWSM) 解决方案

Cisco Secure Firewall Services Module (FWSM)

〔美〕 **Ray Blair**，CCIE #7050
Arvind Durai，CCIE #7016 著

孙余强　李雪峰　译

人 民 邮 电 出 版 社
北　京

图书在版编目（CIP）数据

Cisco安全防火墙服务模块（FWSM）解决方案 /（美）布莱尔（Blair,R.），（美）杜瑞（Durai,A.）著；孙余强，李雪峰译. -- 北京：人民邮电出版社，2011.10
ISBN 978-7-115-26113-7

Ⅰ. ①C… Ⅱ. ①布… ②杜… ③孙… ④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(2011)第152337号

Cisco 安全防火墙服务模块（FWSM）解决方案

◆ 著　[美] Ray Blair　Arvind Durai
译　孙余强　李雪峰
责任编辑　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　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷

◆ 开本：800×1000　1/16
印张：28.5
字数：624 千字　2011 年 10 月第 1 版
印数：1－3 500 册　2011 年 10 月河北第 1 次印刷

著作权合同登记号　图字：01-2009-5769 号
ISBN 978-7-115-26113-7

定价：69.00 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

本书介绍了 FWSM 的软硬件架构，并通过配置案例讲解了 FWSM 的各种部署方式。

本书分为 5 部分，总共 25 章，主要内容有防火墙的类型、FWSM 的概述和运行模式、FWSM 的安全级别和上下文、FWSM 的初始配置和高级配置、FWSM 的设计指导和配置案例，以及 FWSM 4.x 版本中引入的特性和功能等。

本书适合所有打算购买或已经购买 FWSM 安全产品的工程技术人员以及网络维护人员阅读，也适合准备 Cisco 防火墙安全考试的考生阅读。本书同样可以作为高校计算机和通信专业本科生或研究生学习网络安全技术的参考资料。

关于作者

Ray Blair 是一位咨询系统架构师，在 Cisco 已经工作了 8 年之久，主要负责安全和大型网络的设计。他在网络的设计、实施和维护方面有 20 多年的经验，而且该网络几乎囊括了所有的网络技术。他在高科技行业的前 4 年是设计用于过程监控的工业计算机系统。Blair 先生拥有 CCIE 路由和交换、安全，以及 SP 的认证头衔，同时他也是 Novell 认证工程师（CNE）和信息系统安全认证专家（CISSP）。

Arvind Durai 是 Cisco 的一位高级服务技术领导人。他的主要职责是为来自企业、金融、制造业、电子商务、州政府以及卫生保健部门的 Cisco 大客户提供支持。他对安全领域相当关注，并且发表了几篇白皮书和各种不同技术的设计指南。Durai 先生拥有 CCIE 路由和交换、安全认证头衔，并且拥有电子和通信专业的理学学士学位，以及电子工程专业和工商管理专业的硕士学位。

关于技术审稿人

Sunil Wadwani 是 Cisco 安全技术事业部（STBU）的一位技术营销工程师。Sunil 是一位在设计、开发和装备网络产品的技术领域有着 20 年经验的老手。他从 1992 年起加入 Cisco，并作为设计团队的一员开发了 Cisco 7200 路由器的第一个版本。作为一名技术营销工程师，Sunil 如今的职责是就安全产品（如 VPN、防火墙和 IPS）部署的某些方面向客户和销售工程师提供建议。

Sunil 拥有美国加州大学欧文分校的计算机工程硕士学位，以及圣克拉拉大学的 MBA 学位。他与他的妻子 Shalini，以及两个儿子 Shiv 和 Kunal 居住在加利福尼亚的萨拉托加。

Byran Osoro, CCIE No.8548，是 Cisco 的一位系统工程师。在过去 5 年，他服务于小型/中型企业、大型企业以及太平洋西北部的服务提供商网络。他也在 TAC 机构工作过，以对各种技术（包括 PIX 和 VPN 安全设备）提供支持。Osoro 先生曾经负责设计过对可用性和可靠性有着严格要求的高复杂性网络环境，他现在拥有 CCIE 路由和交换、安全、SP 以及语音认证头衔。同时他也是信息系统安全认证专家（CISSP），并且还持有 Juniper 公司认证的互联网高级专员（JNCIS-M）证书。

献词

Ray Blair：本书献给我的妻子 Sonya，我的孩子 Sam、Riley、Sophie 和 Regan。你们就是我的世界！

Arvind Durai：本书献给我的妻子 Monica，在写作本书的漫长时间里，她为我提供了足够的动力和支持，从而保证了本书的顺利完成。我还要把这本书献给我的儿子 Akhhill，他是我完成本书写作的额外能量来源。

谢谢父母提供给我的价值观和机会。

谢谢我的兄弟和他的家人、我的岳父岳母、我的表兄以及他的家人，谢谢他们的支持和祝福。

致谢

Ray Blair:

该项目是一个重要的任务，如果没有下面提及的所有人员的帮助，这将会是一个不可能完成的任务。谢谢你们在本书写作过程中给予的帮助和支持。

我的不懂技术的妻子是本书的第一位审稿人，她遭受了阅读技术资料，查询文理不通的错误和措辞的痛苦，我将会永远记住你对本书成功所做的牺牲和奉献——谢谢你！

谢谢我的孩子 Sam、Riley、Sophie 和 Regan，谢谢你们对我花费大量时间写作本书的忍耐，以及对我“等本书写完后我们就去做”这样的反应的容忍。现在，咱们钓鱼去！

Arvind，你出色的技术知识和我们之间良好的工作关系，使得本书的写作成为一项乐趣。作为你的同事和朋友，为了与你合作，我已经期盼了多年。

Arvind Durai：

谢谢我的妻子，在本书的每一个阶段，她多次审阅了其全部的章节，并给出了改进建议。她常常通宵达旦地与我一起审阅本书，因此我从来没有感到过孤独。谢谢你！

我要感谢 Andrew Maximow（Cisco 高级服务部门的主管）、Uwe Fisher（Cisco 高级服务部门的经理）和 Naheed Alibhai（Cisco 高级服务部门的经理），谢谢他们给予我的支持。我也要感谢那些与我一起进行客户设计的同仁。

Ray，因为这本书，我们之间建立了伟大的合作关系。你卓越的技术知识令人称赞。作为你的朋友和同事，很荣幸能与你一起工作。

感谢在本书的每一个阶段，给予我直接和间接支持的每一个人。没有你们的支持，这本书不可能面世。

特别感谢：

非常感谢 Bryan Osoro 和 Sunil Gul Wadwani。没有他们两位技术评审人员的卓越才华，这本书也不可能面世。

感谢 Cisco 内部的产品开发和测试团队，他们对我们提出的问题进行了解答，并预先发布了用于测试的代码，他们是 Reza Saada、Chandra Modumudi、Donovan Williams、MuninderSambi、Munawar Hossain、Christopher Pagge 和 Ben Basler。

Cisco Press 团队提供了极好的反馈和指导，我们从中受益良多，谢谢 Brett Bartow、Christopher Cleveland、Dan Young 和 Tonya Simpson。

谢谢与我们一起共事的所有客户，每一个客户的场景给了我们创作本书的灵感。

译者序

应编辑之邀翻译本书时，正忙于对《Internet Routing Architectures》(Second Edition)(即《Internet 路由结构（第 2 版)》）的译文做最后的修改和润色，故而只能接手本书第 3、第 4、第 5 部分，即第 12 章～第 25 章的翻译工作。如果读者对这 14 章译文有任何疑问或反馈意见，可发邮件与译者联系。

虽然只接手了本书 14 章的翻译任务，但译者所耗费的精力丝毫不亚于翻译《Internet Routing Architectures》(Second Edition）全书。这是因为本书的两位作者在写作方面似乎是未得其门而入，除了原文语法错误之外，对 FWSM 的许多特性也是语焉不详，翻译时，译者只能反复核查 Cisco 文档，或翻阅 Cisco Press 出版的与 FWSM 相关的图书。除此之外，为了保证译文的准确性，以方便读者理解，译者甚至还“越俎代庖”，替作者添加了不少内容。

当然，这 14 章译文中还是会包含很多译注，其目的只是为了将原作者表达晦涩的意图尽可能准确地传达给读者，从而降低读者的阅读门槛。如果读者之前翻阅过译者翻译的《局域网交换机安全》、《Network Warrior 中文版——思科网络工程师必备手册》等书，就会发现每一本书中都额外添加了许多译者注。当然，如果按照翻译后的中文字数来计算翻译稿酬的话，这么多译者注也可以为我额外换来不菲的收入，可惜的是，出版社是按照原文所包含的英文单词个数来计算稿酬的。

言归正传，译者在翻译完本书 14 章内容后发现，本书两位作者的 CCIE 编号都在 8000 号以内，译者虽不敢妄加评论二位仁兄的技术水平，但行文能力却……哎。也许，这二位仁兄已经准备转行做销售了吧。为此，译者倾注了大量的时间和精力，试图从作者含混残缺的表述中揣测其意图，并力争能够如实传达给读者。这也让译者不由地想起《More Joel on Software》(软件随想录，由人民邮电出版社出版）一书中，作者 Joel Spolsky 给计算机系学生七条建议里的第一条：在毕业前练好写作。在这里，译者真诚建议本书的两位作者，以及有志于从事图书写作的人们，在著书之前还是先好好练习写作吧。

致谢：

感谢傅道坤编辑，感谢你对我的信任。还要感谢你保留译文中所有的译者注，这些译者注是我的心血所在。

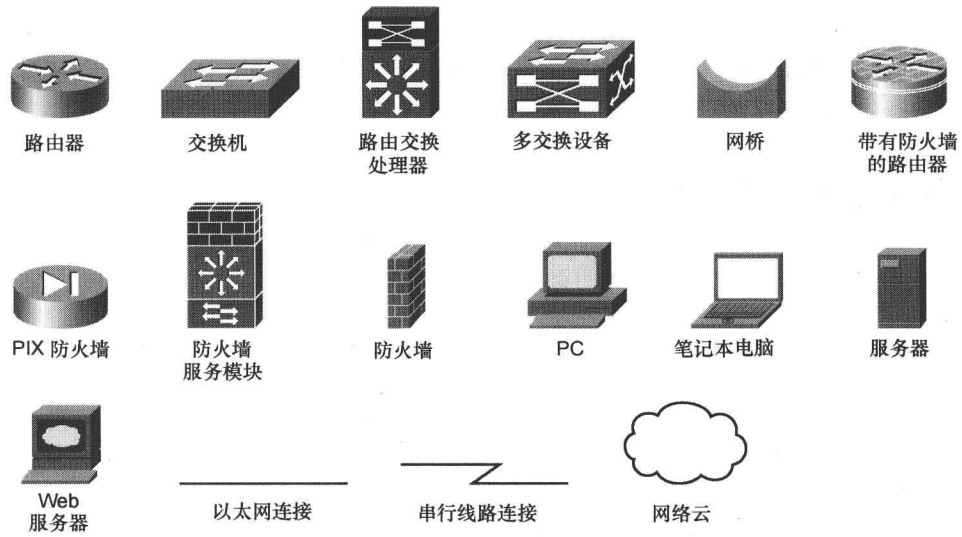
感谢读者 Torrey（torrey_ytang@126.com）（也代表我之前网络技术书籍的合译者孙剑，他赞你是一位真正有耐心去读书的读者），谢谢你指出我们所翻的每一本书中的错误。

感谢 www.56cto.com 的代工（ccie19@163.com），谢谢你指出我之前所翻书籍中的技术错误。

其实，翻译诸如本书二位仁兄所著的书籍，译者不可能从中获得半点益处（无论是从技术上，还是从经济上），不招来骂名已属万幸。如果没有以上二位读者的邮件和傅道坤编辑的再三鼓励，译者也不能支撑下去。

孙余强
sunlengxie@gmail.com
2011 年 6 月 22 日于安徽合肥

本书使用的图标



命令语法约定

本书命令语法遵循的约定与 IOS 命令手册使用的约定相同。IOS 命令手册对这些约定的描述如下。

- **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的参数值。
- 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。

前言

防火墙是一种用来保护网络基础设置的重要组件。要维护一个安全的网络，必须深入理解这些设备的运行机制。

本书从硬件和软件两个角度对防火墙服务模块（FWSM）的功能进行了讲解，同时附带有在不同部署场景中设计、实施、运行和管理 FWSM 的配置案例，因此本书是一本相当实用的 FWSM 设计指导。

本书的读者对象

本书主要针对那些设计、实施或维护 FWSM（如安全/网络管理员）的人员而写。为了能从本书中获取最大收益，读者最好具有至少中级以上的网络和安全知识。

本书的组织结构

本书总共分为 5 个部分，分别为防火墙的基本介绍、初始配置、高级配置、设计指导和配置案例，以及 FWSM 4.x 版本代码中引入的特性和功能。

- **第 1 章，“防火墙类型”**，讲解了不同类型的防火墙的功能。
- **第 2 章，“防火墙服务模块概述”**，讲述了防火墙服务模块的规范、安装信息、性能和虚拟化；对 IOS FW、ASA 和 FWSM 进行了对比；还讲解了防火墙服务模块的硬件和软件架构。
- **第 3 章，“运行模式的分析”**，分析了每一种运行模式（透明/路由）及其各自的优势。
- **第 4 章，“理解安全级别”**，讲解流量如何在使用 NAT 和 PAT 以及路由和透明模式的接口之间流动。
- **第 5 章，“理解 context”**，对 context 的优势和管理方式进行了概述。
- **第 6 章，“6500/7600 系列机箱的配置与保护”**，讲解了如何配置主机机箱来使其支持 FWSM。
- **第 7 章，“FWSM 的配置”**，讲解了 FWSM 的初始配置。
- **第 8 章，“ACL”**，讲解了 ACL 的使用。
- **第 9 章，“路由协议的配置”**，讲解了路由协议在 FWSM 上的使用。
- **第 10 章，“AAA 概述”**，讲解了使用认证、授权和审计（AAA）的原则。
- **第 11 章，“模块化策略”**，讲解了类型和策略映射(map)的使用。
- **第 12 章，“FWSM 中的故障切换”**，讲解了使用多个 FWSM 来提高可用性的应用和配置。
- **第 13 章，“理解应用层协议检测”**，讲解了应用和协议检测的使用以及配置。

- **第 14 章，“流量过滤”**，讲解了如何使用过滤服务器对流量进行过滤，以及 Active X 和 Java 过滤的运行原理。
- **第 15 章，“管理和监控 FWSM”**，讲解了管理和监控 FWSM 的不同选项。
- **第 16 章，“多播”**，讲解了多播与 FWSM 的交互，并提供了几个实际案例。
- **第 17 章，“非对称路由”**，对非对称路由及其配置方式进行了讲解。
- **第 18 章，“防火墙负载均衡”**，讲解了如何使用多个 FWSM 来增强性能的选项。
- **第 19 章，“IP 版本 6”**，对 IPv6 及其在 FWSM 上的配置方式进行了讲解。
- **第 20 章，“网络攻击防护”**，讲解了如何使用规避(shunning)、反欺骗(antispoofing)、连接限制和超时来缓解网络攻击。
- **第 21 章，“排除 FWSM 故障”**，讲解了如何使用适当的工具来解决 FWSM 的故障。
- **第 22 章，“设计网络基础设施”**，对 FWSM 在网络中的放置进行了概述。
- **第 23 章，“设计构思”**，通过多个实际案例来讲解 FWSM 的配置方式。
- **第 24 章，“FWSM 4.x 性能和可扩展性的提升”**，对 FWSM 4.x 代码中性能的改进进行了讲解。
- **第 25 章，“FWSM 4.x 路由功能与其他增强特性”**，对如何使用 FWSM 4.x 代码中引入的命令进行了讲解。

目　录

第1部分　简　介

第 2 部分 初 始 配 置

第 3 部分 高 级 配 置

第 4 部分 设计指导和配置案例