SECURITY

Cisco ASA、PIX与FWSM防火墙手册（第二版）

Cisco ASA, PIX, and FWSM Firewall Handbook

Second Edition

The complete guide to the most popular Cisco ASA 8.0 and FWSM 3.2 firewall security features

〔美〕**David Hucaby,** CCIE #4594 著
罗进文 谭筠梅 饶俊 张媛 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco ASA、PIX与FWSM防火墙手册（第二版）

Cisco ASA, PIX, and FWSM Firewall Handbook

Second Edition

〔美〕David Hucaby, CCIE #4594 著
罗进文 谭筠梅 饶俊 张媛 译

人民邮电出版社
北京

图书在版编目（CIP）数据

Cisco ASA、PIX与FWSM防火墙手册 : 第2版 / (美)赫卡 (Hucaby,D.) 著 ; 罗进文等译. -- 北京 : 人民邮电出版社, 2010.4
ISBN 978-7-115-21861-2

Ⅰ. ①C… Ⅱ. ①赫… ②罗… Ⅲ. ①计算机网络－安全技术－手册 Ⅳ. ①TP393.08-62

中国版本图书馆CIP数据核字(2009)第227766号

版 权 声 明

Cisco ASA、PIX 与 FWSM 防火墙手册（第二版）

◆ 著 [美] David Hucaby，CCIE#4594
译 罗进文 谭筠梅 饶 俊 张 媛
责任编辑 翟 磊

◆ 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
三河市海波印务有限公司印刷

◆ 开本：787×1092 1/16
印张：40.25
字数：1008 千字 2010 年 4 月第 1 版
印数：1－3 500 册 2010 年 4 月河北第 1 次印刷

著作权合同登记号 图字：01-2008-0494 号
ISBN 978-7-115-21861-2

定价：89.00 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

在网络威胁泛滥的今天，利用防火墙技术保护网络的安全已经成为一项极为重要的任务。本书主要内容包括防火墙概述和配置基础、防火墙管理和用户管理、通过防火墙的控制访问、检测流量、使用故障切换增强防火墙的可用性、防火墙负载均衡、防火墙日志、验证防火墙运行、ASA 模块等内容，附录部分还对通用协议和端口号、安全设备日志消息进行了介绍。

本书适合网络管理员、防火墙安全工程师（或顾问）、对防火墙相关技术感兴趣的初学者阅读。

作者简介

David Hucaby，CCIE NO.4594，肯塔基大学杰出的网络工程师，致力于以 Cisco Catalyst、ASA、FWSM 和 VPN 产品线为基础的网络维护，曾是 ASA 8.0 操作系统 beta 版的审查者之一，拥有肯塔基大学的电气工程学士和硕士学位，曾出版过 3 本思科教材：《CCNP BCMSN Official Exam Certification Guide》、《Cisco Field Manual: Router Configuration》和《Cisco Field Manual: Catalyst Switch Configuration》。

现与妻子 Marci 和两个女儿一起居住在肯塔基。

技术支持

Greg Abelar，从 1996 年 11 月至今，一直受雇于 Cisco。他是 Cisco 技术支持安全团队的创始人之一，协助聘用并培训了众多工程师。他在 Cisco 安全架构和安全技术营销工程团队中担任多个职务。他是 Cisco 发起的 CCIE 安全笔试的主要奠基人和项目管理者，曾出版过 Cisco 教材《Securing Your Business with Cisco ASA and PIX Firewalls》，与他人合作出版过《Security Threat Mitigation and Response：Understanding Cisco Security MARS》，并为多本 Cisco 出版的安全类教材担任技术编辑。

Greg Abelar 的博客：

家庭中的 Internet 安全——http://security1a.blogspot.com/；

企业中的 Internet 安全——http://security2b.blogspot.com/。

Mark Macumber，Cisco 销售部系统工程师。1999 年加入 Cisco 后，就职于 ISP 网络的网络服务提供商销售部，致力于电信 DSL 网络设计。2002 年后，他开始服务于大型企业用户，为用户设计校园交换、WAN 路由、统一通信、无线和安全网络。目前，他的技术重点是企业网内的安全产品和架构。企业安全 SE 团队负责学习并实现 Cisco 安全产品，如防火墙、基于入侵检测/防御的主机/网络系统、AAA、安全信息管理、网络准入控制和 SSL/IPSec VPN。

献　辞

与往常一样，我要将此书献给我生命中最重要的人——我的妻子 Marci 和我的两个女儿 Lauren 和 Kara。同时，我也要将此书献给我的父母 Reid 和 Doris Hucaby。

感谢上帝保佑我有一个非常幸福美满的家庭。

致　谢

很荣幸能再次参与 Cisco 出版书籍的编写。对于我来说，尽管编写此书困难颇多，但仍是一件非常有趣的事。在写作过程中 Cisco 出版社的编辑给予了我大量帮助。实际上，我很荣幸能与我的朋友 Brett Bartow 和 Chris Cleveland 又一次共事。他们能力卓越，我将终身难忘！我也要感谢 Mandie Frank 为最后的出版工作做出的贡献。

我要感谢本书的技术支持 Greg Abelar 和 Mark Macumber，感谢他们艰辛的工作和敏锐的洞察力。我非常敬佩他们的能力，也感谢他们自始至终的支持。

还有很多人给了我不遗余力的帮助，不管我认不认识，在此，我将一一列出。

Mark Macumber 是我要好的朋友，在很多方面提供了宝贵的资源。当然，当他看见我表示感谢的 E-mail 时，他有些不好意思了。

我要感谢 ASA 8.0 beta 团队的成员给予我的帮助和指导：Madhusudan Challa、Pete Davis、Matt Greene、Iqlas Ottamalika、Jeff Parker、Priyan Pathirana、Dan Qu、Nelson Rodrigues、Nancy Schmitt、Vincent Shan、Andy Teng、Mark Terrel 和 Nagaraj Varadharajan。

即便我是很晚才加入该 FWSM 3.2 beta 项目，FWSM 3.2 开发小组的成员对我也非常耐心而且友善，他们是 Anne Dalecki Greene、Munawar Hossain 和 Reza Saadat。

感谢 Kureli Sankar 和 Kevin Tremblay 这两位 TAC 工程师，他们为我解答了大量难题。

最后，对我而言，校订本书是一件非常困难的工作。我要感谢 Kara 为我制作并贴满屋子的便条，有两个便条至今让我印象深刻：“太晚了”和“懂得感恩”。

序　言

当今的网络要求能将数据、语音、视频会议、无线通信及更多方面的内容安全传输到诸如雇员、供应商、合作伙伴和客户之类的广泛用户。保护网络的安全已经成为一项极为重要的任务，应能保证“无处不在的连接”不会受到网络上未验证访问、滥用或攻击风险的影响而正常地运行。

当各种数量庞大的安全技术应用到安全网络和终端问题上时，具有长期可靠性的防火墙仍然是所有安全部署的核心部分。防火墙继续承担主要的网守任务，确保所有从第 2 层到第 7 层的网络流量经合法验证、授权后传输到网络。

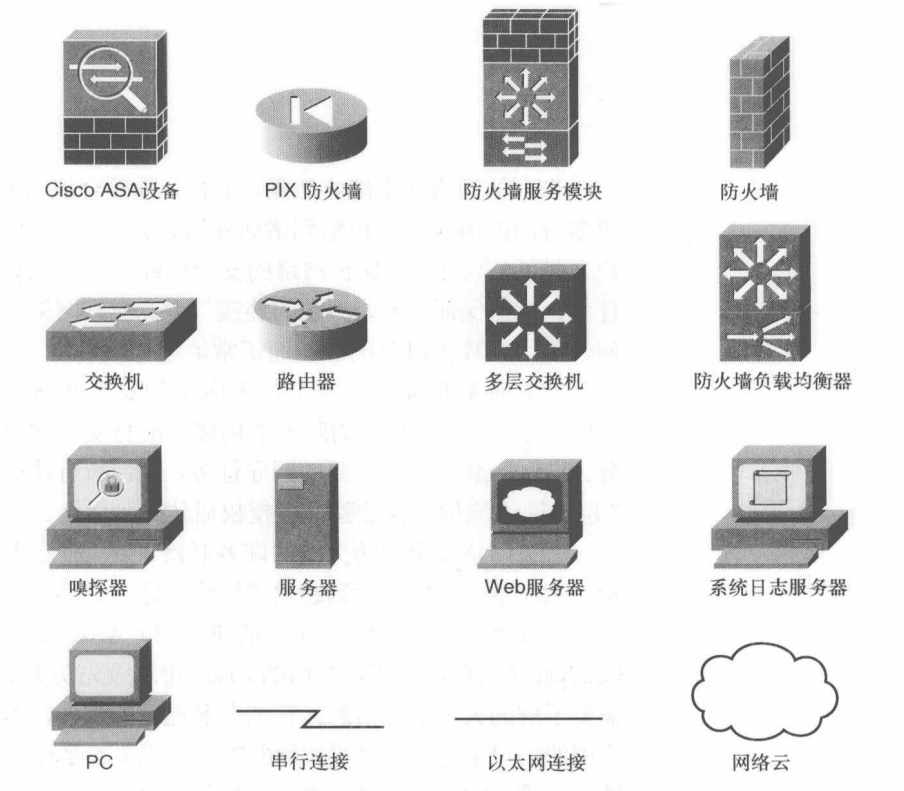
有关网络安全和防火墙的许多书籍主要关注的是概念和理论。然而本书的内容远远超出了这些主题，它涵盖了每个网络和安全管理员在配置和管理包括 PIX 和 ASA 安全设备以及 Catalyst 防火墙服务模块在内的 Cisco 市场领先防火墙产品时，需要了解的大量细节信息。正如书名提示的那样，本书是一个实用的用户手册，提供对初始配置，更重要的是对 Cisco 防火墙日常管理的深入解释。本书对如何成功配置防火墙包括建立访问控制策略、验证终端用户、调节高可用性部署、通过大量管理界面监控防火墙健康在内的所有方面，提供了日常的实践指导。

本书的作者，CCIE David Hucaby 在充当肯塔基大学（University of Kentucky）管理 Cisco 防火墙的首席网络工程师之余，还花费了相当多的时间直接与负责这些产品的 Cisco 工程小组协作，确保本书涵盖了深入、实用、最新的可用信息。将本书放在手边——你会发现经常需要参考它！

Jason W. Nolet
工程部副总裁
安全技术组
Cisco
2007 年 6 月

本书图标使用说明

纵观本书，你会发现一些用于表示 Cisco 和普通网络设备、边缘设备和其他设备的图标。以下的图标说明解释了这些图标含义。



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

本书主要针对的是Cisco防火墙硬件整个产品系列：PIX、ASA 安全设备系列和 Catalyst 防火墙服务模块（FWSM，Firewall Services Module）。涵盖了Cisco防火墙众多的信息和文档资源，另有一些快速、简便的解决方案。

本书致力于为能在Cisco防火墙中配置的全部特性提供快速、简便的参考指南。实际上，防火墙的所有文档和其他网络设计的参考材料都已被压缩到一个手册中。

本书仅包含能用于全状态流量检测和全网安全的特性。尽管Cisco防火墙也支持VPN功能，但本书不包含这些内容。

本书基于目前最常见的 Cisco 防火墙软件版本——ASA 8.0版和FWSM 3.2(1)版。

你可在本书中发现ASA、PIX和FWSM命令一同出现在特定的任务中。根据以下约定，所示带标记的命令语法表明这类软件正在运行。

- **ASA**——指任何可以运行ASA 7.0版或更高版本的平台，包括ASA 5500和PIX 500系列产品。例如，尽管PIX 535可运行ASA 8.0版，此命令仍标记为“ASA”，以便与所使用的操作系统相一致。
- **PIX**——指PIX 6.3版。
- **FWSM**——指FWSM 3.1版或更高版本。

如果你正使用的软件是早期版本，你会发现配置命令有细微的差别。

随着ASA平台的出现，Cisco开始使用不同的术语：由于软件带有大量安全特性和ASA机架的模块特性，防火墙开始被称为*安全设备*。本书将这个新术语在适当的部分进行合并。但是，术语*防火墙*仍是出现最频繁的词汇，这是因为本书既涉及安全设备，又涉及嵌入Catalyst交换机机架的防火墙。当你阅读本书时，请记住术语*防火墙*和*安全设备*是等价的。

本书的内容结构

无论你是网络或安全管理员、工程师、顾问还是学生，本书都可以成为你日常工作中的工具书。我尝试对众多防火墙特性进行透彻的解释。当你理解了防火墙的工作原理后，你能更容易配置防火墙，并进行故障排除。

本书按对各种 Cisco 防火墙特性的简介、配置步骤、配置选项的解释分为不同的章节。各章节和附录如下所示。

- **第 1 章　防火墙概述**——介绍 Cisco 防火墙的流量检测原理。同时提供了多种防火墙模型及其性能的简明信息。
- **第 2 章　配置基础**——讨论 Cisco 防火墙的用户接口、特性设置和配置方式。
- **第 3 章　建立连接**——阐述如何配置防火墙接口、路由选择、IP 寻址服务和 IP 组播支持。
- **第 4 章　防火墙管理**——阐述如何配置并维持安全 context、Flash 文件和配置文件，如何管理用户，以及如何用 SNMP 监控防火墙。
- **第 5 章　防火墙用户管理**——包含用于对防火墙管理员和终端用户进行验证、授权并维持统计记录的各种方法。
- **第 6 章　通过防火墙的控制访问**——介绍运行和配置透明或路由模式的防火墙、地址转换、流量规避和威胁检测。
- **第 7 章　检测流量**——涵盖用于定义安全策略的模块化策略架构，可识别并对各类流量进行操作。本章也讨论了安全策略所使用的应用层检测引擎和内容过滤。
- **第 8 章　使用故障切换（failover）增强防火墙的可用性**——阐述防火墙故障切换的运行和配置，一组防火墙协同运行可提供高可用性。
- **第 9 章　防火墙负载均衡**——讨论防火墙负载均衡的工作原理，如何在网络中实现此特性，以便在防火墙群中穿过众多防火墙分发流量。
- **第 10 章　防火墙日志**——阐述如何配置防火墙来产生动态登录消息，以及如何分析登录消息的内容。
- **第 11 章　验证防火墙运行**——包含如何通过检查防火墙的生命特征来确定其健康状况，如何验证其有效性，以及如何观察流经防火墙的数据。
- **第 12 章　ASA 模块**——讨论可被增加到 ASA 机架中的安全服务模块(Security Services Module，SSM)，及其基本的配置和使用。
- **附录 A　通用协议和端口号**——列出防火墙配置命令支持的已知 IP 协议号、ICMP 消息类型和 IP 端口号。
- **附录 B　安全设备日志消息**——将由 ASA、PIX 或 FWSM 防火墙产生的众多日志消息整理为一个简明参考手册。

阅读指南

本书中的信息遵循简明参考手册的格式。如果你已掌握所使用的防火墙特性或技术，可直接进入对应的章节。主要章节已按简明参考手册索引进行编号，带有各自的章节号（例如，

3.3 表示第 3 章第 3 节）。每页的阴影索引列出了对应的章节号。

特性描述

各主要章节的开头均有特性的详细解释或简明列表。从这些信息中可快速学习或回顾这些特性的原理。

配置步骤

包含在各章中的特性均有必需或可选的配置命令。配置步骤的不同之处均以概要形式表示。如果你遵照这些概要，你可以配置复杂的特性或技术。如果你不需要某种特性选择，可以直接跳过这一级的概要。

在某些章节，你会发现在配置概要中的每一个步骤将多个防火墙平台中的命令简要地并排列出。所以，无论你面对的何种类型或模式的防火墙，你都可以翻阅相同的配置章节。

配置实例

每个章节都通过一个实例来阐述如何执行命令及其选项。各实例都夹杂在配置步骤中和主要章节的末尾。我努力尝试让你在学习这些实例时，所输入的命令是按照概要的顺序进行的。

大多数时候，由于命令是按预先定义好的顺序来显示，而不是按照你输入的顺序，所以难于学习和理解。如果有可能，本书中的实例也仅显示对应章节的命令。

相关特性的显示信息

你可以使用一些命令来显示防火墙的特性，各章节都包含这类命令的显示信息。我希望通过这类实例的输出，来帮助你解释防火墙中相同的输出。

本章包含以下内容。

- **防火墙运行概述**：讨论用于检测和控制通过 Cisco 防火墙流量的机制。防火墙检测引擎和算法负责将安全策略配置注入防火墙。
- **ICMP、UDP 和 TCP 的检测引擎**：描述防火墙如何对不同 IP 协议的流量进行响应。涉及对 ICMP、UDP 和 TCP 协议的检测机制。
- **硬件和性能**：对各种 Cisco 防火墙平台及其规范进行概述和比较。这些内容可以帮助你决定哪种防火墙模式最适合于你的应用。
- **基本安全策略准则**：对一个公司网络中防火墙配置和维护的一些建议。

目 录