SECURITY

Cisco ASA设备使用指南

Cisco ASA

All-in-One Firewall, IPS, Anti-X, and VPN
Adaptive Security Appliance
Second Edition

Identify, mitigate, and respond to network attacks

〔美〕 **Jazib Frahim**，CCIE #5459
Omar Santos 著

田果，CCIE #19036
刘丹宁，CCIE #19920 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco ASA设备使用指南

Cisco ASA

All-in-One Firewall, IPS, Anti-X, and VPN
Adaptive Security Appliance
Second Edition

〔美〕 **Jazib Frahim**，CCIE #5459
Omar Santos 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

Cisco ASA设备使用指南 / (美) 弗拉海(Frahim, J.), (美) 桑托斯 (Santos, O.) 著 ; 田果译
-- 北京 : 人民邮电出版社, 2010.11
ISBN 978-7-115-23437-7

Ⅰ. ①C… Ⅱ. ①弗… ②桑… ③田… Ⅲ. ①计算机网络－安全技术－指南 Ⅳ. ①TP393.08-62

中国版本图书馆CIP数据核字(2010)第142221号

版 权 声 明

Cisco ASA 设备使用指南

◆ 著 [美] Jazib Frahim，CCIE#5459 Omar Santos
译 田 果，CCIE#19036 刘丹宁，CCIE#19920
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 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京铭成印刷有限公司印刷

◆ 开本：787×1092 1/16
印张：51.25
字数：1383 千字 2010 年 11 月第 1 版
印数：1－3 500 册 2010 年 11 月北京第 1 次印刷

著作权合同登记号 图字：01-2010-0306 号
ISBN 978-7-115-23437-7

定价：108.00 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

这是一本全面介绍 Cisco ASA 部署方法的图书，它的主要内容有：安全技术简介；ASA 系列产品的产品线、如何初始化 ASA 系统；如何在 ASA 上配置防火墙技术（包括访问控制列表、IP 路由、AAA 技术、应用层监控、虚拟防火墙、透明防火墙、故障倒换与冗余以及服务质量）、IPS 技术、内容安全技术及 VPN 技术（包括站点到站点 IPSec VPN、IPSec 远程访问 VPN、PKI 以及远程访问 SSL VPN）；除此之外，本书还介绍了如何对 ASA 上的配置进行验证等。本书介绍的配置案例相当丰富，配置过程相当具体，它几乎涵盖所有使用了 ASA 系列产品的环境。

本书适合所有准备购买或已经购买 ASA 系列产品的网络技术人员阅读，也适合需要对各类安全产品进行测评的相关人士阅读。除此之外，本书还适合正在准备参加 CCNA 安全（640-553）、SNAF（642-524）、SNAA（642-515）、CCIE 安全笔试（350-018）以及 CCIE 安全实验考试的考生阅读。鉴于本书所介绍的内容由易到难，因而它的内容可以满足各类 ASA 用户的不同需要，也适合正在准备各类 Cisco 防火墙安全考试的考生进行参考阅读。

关于作者

Jazib Frahim，CCIE No.5459，加盟 Cisco Systems 已超过 10 年，拥有伊利诺斯理工学院的计算机工程学士学位。在加盟 Cisco 之初，担任 LAN 交换小组的 TAC 工程师，而后进入了 TAC 安全小组并担任安全产品的技术负责人。他领导的小组由 20 位工程师组成，专司解决复杂的安全和 VPN 技术问题。目前，他是 Worldwide Security Services Practice of Advanced Services for Network Security 的技术负责人，负责指导客户设计并实施网络，并主要关注网络安全方面。他拥有两个 CCIE 认证，一个是路由交换方向，另一个是安全方向。他撰写了很多 Cisco 在线技术文档，同时也是 Cisco 在线论坛 NetPro 的活跃会员。他曾多次出席 Networkers 大会，并为 Cisco 客户、合作伙伴和员工主讲多门现场和网络课程。

在供职 Cisco 期间，他获得了北卡罗来纳州立大学的工商管理硕士（MBA）学位。

他还为 Cisco Press 撰写了如下著作。

《Cisco ASA：All-in-One Firewall，IPS, and VPN Adaptive Security Appliance》

《Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting》

《SSL Remote Access VPNs》（该书中文版已由人民邮电出版社引进出版）

Omar Santos 是 Cisco 产品安全事故响应小组（PSIRT）的事故经理。Omar 曾为多家世界 500 强企业以及美国政府进行过安全网络的设计、实施和维护工作，其中也包括美国海军陆战队（USMC）和美国国防部（DoD）的网络。他同样是很多 Cisco 在线技术文档及配置指导的作者。在担任现在的职务之前，他曾是全球安全事务组及 Cisco 技术支持中心（TAC）的技术负责人，在此期间，他曾教授、带领并指导了上述两个部门的多位工作师。

Omar 也曾为 Cisco 客户和合作伙伴做过多次技术演讲，并为许多企业的 CEO、CIO 和 CSO 等高层主管进行过多次演讲。同时，他曾为 Cisco Press 撰写了以下著作。

《Cisco ASA：All-in-One Firewall，IPS, and VPN Adaptive Security Appliance》

《Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting》

《End-to-End Network Security: Defense-in-Depth》

关于技术审校人

Randy Ivener，CCIE No.10722，是 Cisco 安全研究与操作小组的安全工程师。他还是一名 CISSP 和 PMI PMP。他曾多年担任网络安全顾问，并帮助很多企业了解和保护他们的网络。Randy 曾经在包括 Blackhat 和 Cisco Networkers 在内的许多会议上进行过以安全为主题的演讲。在涉足信息安全领域之前，他曾从事过软件研发并担任培训师之职。Randy 毕业于美国海军学院，并拥有 MBA 学位。

Jay Johnston，CCIE No.17663，是北卡罗来纳州三角研究园 Cisco TAC 中心的一位安全专家。他自 2002 年开始投身网络事业，当时他以合作教育的身份加盟了 Cisco 并同时进入北卡罗来纳州立大学学习。他在 2004 年获得了计算机科学学士学位，同时作为全职 TAC 工程师加盟 Cisco，并在 2007 年获得 CCIE 安全认证。他十分热爱 Cisco 的工作，这是因为 TAC 这个职位可以让他长期面对来自客户的技术挑战。

献辞

Jazib Frahim：愿将本书献给我挚爱的妻子 Sadaf，在我撰写本书期间，她表现出来的耐心和宽容使我深受鼓舞。

同时，我愿将本书献给我的父母 Frahim 和 Perveen，我的每次拼搏背后都少不了他们的鼓励与支持。

最后，我要感谢我的兄弟姐妹们，包括我的哥哥 Shazib、姐姐 Erum 和 Sana、嫂子 Asiya、可爱的侄子 Shayan 及侄女 Shiza 和 Alisha。感谢你们在我写作本书时给予的理解与支持。

Omar Santos：愿将本书献给我挚爱的妻子 Jeannette，以及我可爱的女儿 Hannah 和儿子 Derek，你们的支持和鼓励是我写作本书的源动力。

另外，我愿将本书献给我的父母 Jose 和 Generosa。没有你们的博学、睿智和引导，我将永远无法成就今天的高度。

致谢

谨在此感谢本书的技术编辑 Randy Ivener 和 Jay Johnston，他们付出的时间和给予的技术指导使我们获益良多。他们对我们的作品进行了审校，并纠正了许多大大小小难以发现的错误。特别要感谢 Aun Raza，他在最后一次编辑之前审核了本书的很多章节。

我们还要感谢 Cisco Press 小组，特别是 Brett Battow、Dayna Isley、Kimberley Debus 和 Andrew Cupp，他们的耐心、指导和关爱，他们的每一分努力都值得铭记在心。

非常感谢我们的 Cisco 管理组，包括 David Philips、Ken Cavanagh 和 Jean Reese，本作的面世和他们的支持与鼓励是分不开的。

我们还要对这款由 Cisco ASA 产品研发小组开发的产品表示由衷赞赏。另外，在写作本书的过程中，也离不开他们的支持。

最后，感谢 Cisco TAC。这里孕育了网络工程领域中，无数最光辉、最伟大的思想。为 Cisco 客户提供支持往往将我们置于强大的压力之下，因此这里每天都有奇迹诞生。TAC 工程师是真正的无名英雄，对我们来说，能够与他们并肩作战就是至高无上的荣耀。

译者序

从书名中不难发现，本书与 Cisco Press 出版的图书有很大不同：它不是围绕着某一类特定的技术进行介绍，而是围绕 Cisco 的一个产品系列展开的。

Cisco ASA 系列产品虽然在操作方式上与 Cisco 生产的路由器、交换机有很大的共通之处，但是作为专业的安全类产品，它毕竟涵盖了许多路由交换类产品并不支持的特性、功能和用法。因此，有些熟稔 Cisco 路由交换类产品操作方式的工程师，在面对 Cisco ASA 系列产品时，也会显得一筹莫展。在我们接触过的项目中，这样的案例屡见不鲜。

因此，这本书的出现可谓及时，它非常全面地介绍了 ASA 的各类应用场景，及实施、部署的方法。更为难得的是，本书还对 ASA 的不同型号、操作系统的不同版本，乃至各类硬件模块分别用不同的方式进行了介绍，有的寓于配置案例的分析之中，有的则长篇累牍地进行了对比和分析。

总之，这本书完全可以看作是 ASA 的使用说明书，对于 ASA 产品的用户来说，它的意义和作用不言自明。对于正在使用其他厂商同类产品的用户来说，它也极具参考价值。

必须指出的是，本书是我们翻译过的部头最大的专业图书，尽管诚惶诚恐、甚至几经拖稿，但是错误和疏漏仍然无法避免。为了尽可能弥补有可能出现的错误，我们会在最后留下自己的联系方式，欢迎读者（亦包括《网络安全技术与解决方案》（修订版）及《MPLS 和 VPN 体系结构》（重译版）的读者）在发现问题之后积极与我们进行沟通。当然，如果偶遇不方便接听电话的情况，也请读者予以理解。

最后，我们要感谢 YesLab（http://www.yeslab.net）的秦柯老师（现任明教教主），他在本书的翻译过程中为我们提供了莫大的帮助和支持。

田果
电话：13522498333
邮箱：thesmilingorbit@gmail.com
刘丹宁
邮箱：danning.bj@gmail.com

本书中使用的图标

命令语法约定

本书中用于表示命令的语法约定与 IOS 命令参考手册中使用的一样。命令参考手册描述的约定如下。

- 用**粗体**字表示按字面显示输入的命令和关键字；在实际的配置范例和输出中（非通用命令语法中），粗体字表示用户手工输入的命令（比如 **show** 命令）。
- 用*斜体*字表示必须提供的实际值或参数。
- 用竖线（|）隔开互斥的参数。
- 用方括号（[]）表示可选的参数。
- 用（{}）表示必不可少的选项。
- 用（[{}]）表示可选参数中必不可少的选项。

前言

对于那些不能分别部署防火墙、入侵防御、虚拟专用网络服务设备的企业来说，网络安全始终是一个亟待解决的问题。Cisco ASA 是一款高性能、多功能的安全设备，它可以提供防火墙、IPS、网络防病毒及 VPN 服务。Cisco ASA 集多种功能于一体，兼备快速回复及强大的扩展性，同时还可以提供以上所有特性。

本书可以为业内人士在对 Cisco 自适应安全设备进行设计、实施、配置和排错时，提供指导。它可以站在资深 Cisco 网络安全咨询工程师的角度，给读者提供很多专家级的指导。它阐释了 Cisco ASA 上的自适应身份识别及威胁缓解技术如何能够为大中小各类企业提供各种纷繁芜杂的网络安全解决方案。本书还假定了各类读者有可能遇到的问题，并提供了解决方案，这些问题从实现基本网络安全策略到实施高级的 VPN 和 IPS 服务，不一而足。

谁应该阅读本书

本书旨在为管理网络安全的人员或安装、配置防火墙、VPN 设备或入侵检测/防御系统的专业人士提供技术指导。本书的主题围绕着从初级到高级的网络安全和 VPN 技术进行了介绍。本书的读者应具备一些基本的 TCP/IP 和网络互联方面的知识。

本书是如何组织的

本书分为 5 个部分，先对 Cisco ASA 产品进行了介绍，然后分别对防火墙特性、入侵防御、内容安全和 VPN 进行了介绍。其中每一部分都包括了很多的配置实例，以及对设计方案的深入分析。通过我们为各项技术提供的多种调试结果，读者可以强化自己的学习效果。另外，本书还介绍了很多创新技术，如 SSL VPN、虚拟防火墙以及第 2 层防火墙。

- 第 1 部分“产品概述”包括以下章节。
  - 第 1 章“安全技术介绍”——本章对 Cisco ASA 所支持的不同技术，以及时下被网络安全从业人员广泛应用的技术进行了概述。
  - 第 2 章“Cisco ASA 产品及解决方案概述”——本章介绍了 Cisco ASA 是如何从其他安全产品中吸收各类技术，并将防火墙、入侵检测与防御及 VPN 技术集于一身的。另外，本章还对 Cisco ASA 的硬件进行了概述，包括具体的技术说明和安装指导的。本章还介绍了自适应监控与防御安全服务模块（AIP-SSM）和内容安全与控制安全服务模块（CSC-SSM）。
  - 第 3 章“初始设置及系统维护”——本章全面罗列了初始化设置任务和系统维护流程。准备安装、配置和管理 Cisco ASA 的业内人士，需要执行这些任务，并遵循相应的流程。
- 第 2 部分“防火墙技术”包括以下章节。
  - 第 4 章“控制网络访问”——Cisco ASA 可以保护一个或多个网络，使其免受入侵者的危害。这些网络之间的连接可通过高级防火墙功能进行严密的控制，这可以确保从受保护网络中流入和流出的流量必须遵循企业的安全策略。本章为读者展示了如何通过 Cisco ASA 提供的特性来实施企业的安全策略。

- 第 5 章“IP 路由”——本章介绍了 Cisco ASA 的各项路由功能。
- 第 6 章“认证、授权和审计（AAA）”——Cisco ASA 支持大量的 AAA 特性。本章介绍了如何定义并运用一系列认证方式，以此对 AAA 服务进行配置。
- 第 7 章“应用监控”——Cisco ASA 状态化应用层监控可以保护网络中的应用和服务。本章介绍了如何使用和配置应用监控。
- 第 8 章“虚拟防火墙”——Cisco ASA 虚拟防火墙特性引入了在同一个硬件平台上运行多个防火墙实例（虚拟防火墙）的概念。本章介绍了如何对所有这些安全虚拟防火墙进行配置和排错。
- 第 9 章“透明防火墙”——本章介绍了 Cisco ASA 中的透明（二层）防火墙模式。它介绍了用户如何在透明单防火墙和多防火墙模式下对 Cisco ASA 进行配置，以满足他们的安全需求。
- 第 10 章“故障倒换与冗余”——本章介绍了 Cisco ASA 提供的各类故障倒换和冗余机制。本章不仅包括了它们的概述及配置，也具体介绍了排错的流程。
- 第 11 章“服务质量”——QoS 是一种网络特性，可使管理员为特定类型的流量设置优先级。本章介绍了如何在 Cisco ASA 中对 QoS 进行配置和排错。

- 第 3 部分“入侵防御系统（IPS）解决方案”包括以下章节。
  - 第 12 章“IPS 配置与排错”——入侵检测与防御系统可以保护网络免受来自内部和外部的攻击及威胁，因此可以提供比防火墙更高级的保护功能。本章介绍了 Cisco ASA 中的入侵防御系统（IPS）特性，同时对配置 AIP-SSM IPS 软件的方法提供了专家级的指导。另外，本章提供的排错方案可以提升读者的学习效果。
  - 第 13 章“IPS 调试与监测”——本章介绍了 IPS 的调试进程，以及监测 IPS 事件的最佳方法。
- 第 4 部分“内容安全”包括以下章节。
  - 第 14 章“Cisco 内容安全和控制安全服务模块”——内容安全与控制安全服务模块（CSC-SSM）用于检测病毒、蠕虫、木马及其他安全威胁，并对其采取措施。它可以对 SMTP、POP3、HTTP、FTP 网络流量进行监控。本章介绍了在企业中成功部署 CSC-SSM 的配置和排错指导方针。
  - 第 15 章“Cisco 内容安全和控制安全服务模块的监测与排错”——本章介绍了在对 CSC-SSM 进行监测的最佳方式，以及对所有有可能遇到的问题进行排错时，管理员应当采取的方法。
- 第 5 部分“虚拟专用网（VPN）解决方案”包括以下章节。
  - 第 16 章“站点到站点 IPSec VPN”——Cisco ASA 可支持 IPSec VPN 特性，允许用户从不同地理位置连接到企业网络。本章介绍了成功部署站点到站点 IPSec VPN 的配置和排错指导方针。
  - 第 17 章“IPSec 远程访问 VPN”——本章介绍了两种 Cisco ASA 可支持的远程访问 VPN 解决方案（Cisco IPSec 和 L2TP over IPSec），同时提供了大量配置案例和排错场景。
  - 第 18 章“公钥基础（PKI）”——本章从介绍 PKI 的概念开始，逐步覆盖 Cisco ASA 中的 PKI 配置及排错。
  - 第 19 章“无客户端远程访问 SSL VPN”——本章提供了 Cisco ASA 中无客户端 SSL VPN 功能的详细介绍。本章详细介绍了 Cisco 安全桌面（CSD）解决方案，以及用于收集终端工作站状态信息的主机扫描（Host Scan）特性，同时还提供了动态访问

策略（DAP）特性的用途以及详细的配置案例。为了加强学习效果，本章随同配置步骤提供了诸多不同的部署场景。

- 第 20 章“基于客户端的远程访问 SSL VPN”——本章提供了 Cisco ASA 中基于客户端的 SSL VPN 功能的详细介绍。

目　录

第1部分　产品概述

第 2 部分　防火墙技术

第 3 部分 入侵防御系统（IPS）解决方案