CISCO SYSTEMS

ciscopress.com

Cisco 路由器防火墙安全

Cisco Router Firewall Security

Harden perimeter routers with Cisco firewall functionality and features to ensure network security

[美] Richard A. Deal 著
陈克忠 译

人民邮电出版社
POSTS & TELECOM PRESS

Cisco 路由器防火墙安全

[美] Richard A. Deal 著

陈克忠 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

Cisco 路由器防火墙安全 /（美）迪尔（Deal, R. A.）著；陈克忠译.
—北京：人民邮电出版社，2006.1

ISBN 7-115-13695-5

Ⅰ. C... Ⅱ. ①迪...②陈... Ⅲ. 计算机网络—防火墙 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 126386 号

版 权 声 明

Cisco 路由器防火墙安全

◆ 著 [美] Richard A. Deal
译 陈克忠
责任编辑 李 际

◆ 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
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：43
字数：1 056 千字 2006 年 1 月第 1 版
印数：1–3 000 册 2006 年 1 月北京第 1 次印刷

著作权合同登记号 图字：01-2005-0798 号

ISBN 7-115-13695-5/TP • 4815

定价：98.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223

内容提要

本书全面系统地介绍基于 Cisco IOS 软件操作系统的各种防火墙特性。使用这些特性可以加固 Cisco 边界路由器和其他路由器，在保护已有投资的情况下，保护我们的网络免受各种安全威胁和攻击。

本书共有 21 章，分成 9 个部分。第一部分是安全问题和防火墙的概述。第二部分通过基本的访问设置、关闭不必要的服务和实施 AAA 来保护到路由器本身的访问安全。第三部分介绍 Cisco 的无状态流量过滤技术，包括基本的、扩展的、命名的、定时的、有序的和编译的 ACL。第四部分介绍 Cisco 的有状态的流量过滤技术，包括反射 ACL、CBAC、URL 过滤和 NBAR 等特征。第五部分介绍地址转换和地址转换所引起的问题以及相应的解决方法。第六部分分别介绍锁和密钥 ACL、认证代理和对路由选择协议的保护，锁和密钥以及认证代理用来实现在允许用户访问资源之前首先对他们进行认证的功能。第七部分主要介绍入侵检测系统、DoS 防护和记录日志事件。第八部分介绍站到站的 IPSec 连接和远程接入 IPSec 连接。第九部分介绍一个综合的案例学习，结合本书中介绍的重要安全组件，讲述如何保护一个实际环境中的网络安全。

本书是一本关于“如何做”的书，堪称是一部关于 Cisco 路由器防火墙安全的参考大全。作者 Richard 是一位有多年计算机网络业工作经验的专家，本书融入了作者网络安全实践的很多体会和提示，使读者能更好地掌握重要特征和关键问题。本书中提供的许多例子都很典型，可以方便地应用到我们的网络环境中。本书文笔流畅、内容翔实、覆盖面很广，是广大网络安全从业人员和网络管理人员的案头必备用书。本书也可以有效地帮助您通过 Cisco 的 CCSP SECUR 认证考试。

关于作者

Richard A. Deal 拥用 CCSP, CCNP 和 CCNA 证书，曾经就读于 Grove 市立学院，他主修数学、计算机和英语，并获得科学学士学位。在过去的 7 年里，Richard 经营他自己的公司，该公司提供咨询和技术培训。Richard 在计算机和网络业（包括网络、培训、系统管理和编程）有 17 年的工作经验。

除了教授各种 Cisco 的认证课程之外，Richard 已经出版了很多本书，最近出版的是 *CCNP BCMSN Exam Cram 2*（642-811），由 Que 出版社出版。Richard 正在为 Boson 公司撰写 Cisco 认证自我准备测试，包括 SECURE 测验（SECURE #3）。Boson 软件公司是一家软件和培训公司，专门从事考试准备和动手技能产品的开发。Boson 作为一家赢利的软件公司，自 1998 年以来一直关注成人学习和网络公共事业。他们的使命是以经济有效的方式提供高质量的实践测试和学习补充材料。Boson 是支持 Cisco 认证的第一批软件供应商之一，现在是 Cisco 授权的学习合作伙伴和产品总代理。Boson 的其他学习帮助材料可从 http://www.boson.com 获得。

Richard 和他的妻子 Natalie 以及刚出生的女儿 Emily 目前生活在佛罗里达州的奥维耶多市，在奥兰多的旁边。

关于译者

陈克忠，CCNA，CCNP，长期从事 Cisco 网络的设计、部署、维护和安全优化，具有多年电信级大型网络实践经验，并长期担任 Cisco 网络安全课程讲师和几家企业的安全顾问。另有译著《CCSP 自学指南：安全 Cisco IOS 网络（SECUR）》。

关于技术审稿人

Scott Clayton（CCIE No.10064）是一位系统工程师，专门研究安全和 VPN 设计。他当前的工作是为几家财富 100 强公司提供支持，还有一些本地的和州政府客户。在担任这个职位之前，Scott 在 Cisco 公司技术支持中心工作，在安全、VPN 以及内容服务产品和技术等很广的范围内为客户提供支持。Scott 是在 2002 年 10 月参加并通过 CCIE 安全考试的第一批专家之一。Scott 从弗吉尼亚州的威廉斯堡市的威廉&玛丽学院获得科学学士学位。

Stephen Marcinek（CCIE No.7225）是 Boson 培训公司的技术教师。他开发课程内容并开了关于 Cisco 网络和安全方面的大量课程，这些课程包括从入门级别到 CCIE 级别。Steve 也为许多大型公司提供咨询。他从鲁斯大学获得了艺术学士学位，是美国门撒国际的一名成员。

Umar Shafiq（CCIE No.7119）自 1998 年以来，一直在 Cisco 公司工作，担任客户支持工程师。他的团队在全世界范围内为所有已安装的 Cisco 设备做多协议网络、网络安全和 VPN 方面的高端技术排错。他在巴基斯坦的拉合尔科学技术大学电子工程系获得了科学学士学位，并在加利福尼亚州立大学获得了硕士学位。他目前居住在加利福尼亚的弗里蒙特。

献　词

本书献给 Natalie 和 Emily。感谢你们给我的生活带来了那么多的欢乐。

致　谢

我要特别感谢 Cisco Press 的 Michelle Grandin，给了我编写这本书的机会，也要感谢 Cisco Press 的团队，他们让本书的撰写进行得非常顺利。

特别感谢本书的技术编辑：Umar Shafiq、Scott Clayton，尤其是 Steve Marcinek。我个人认识 Steve 已经有段时间了，作为一位合作者和朋友总是能依靠他。

非常感谢本书的生产团队。Marc Fowler 和 Krista Hansing 非常专业，很高兴能和他们一起工作。特别衷心地感谢 Drew! 我可能找不出比他们更优秀的团队。

最后也是最重要的是，如果没有我的妻子 Natalie 的支持，本书就不可能出版。如此篇幅的一本书是很耗费时间的，尤其是还要平衡用在写书、工作和最重要的家庭之上的时间。当我被迫在截稿时间之内完成本书时，我的妻子给了我无尽的鼓励，帮助我坚持写作。

祝大家好运！

前　言

多年来，Cisco 已经是网络业的一个重要组成部分，并继续变得更重要。早在 1993 年，作者使用的第一台路由器产品是 Cisco AGS+。作者看到过 Cisco IOS 软件的很多特性，包括今天我们在 Cisco IOS 软件操作系统中引入的绝大多数安全特性。过去几年中，作者看到安全正成为网络设计中的一个关键组件。当今，随着更多的公司将 Internet 用作业务工具，安全显得比以前更重要了。

目标和方法

3 年前，作者认识到有很多认证方面的书可以帮助技术人员通过 Cisco 的安全认证考试，但是没有任何一本书的内容将 Cisco 的所有安全特征集中应用到一个实际中。作者经常查看各种 Cisco 新闻组，经常看到有关如何实施各种 Cisco 安全特征的问题。这是作者写第一本安全著作 *Cisco PIX Firewalls* 的初衷。

写作这本《Cisco 路由器防火墙安全》的目的是，介绍如何使用 Cisco 路由器实施边界防火墙解决方案。从头到尾，本书关注 Cisco IOS 软件的重要特性，以及如何使用它们来保护我们的边界路由器，并为出入网络边界的流量提供一个安全的解决方案。当然，本书中讨论的很多主题都可以被应用到网络中的任何 Cisco 路由器；然而，因为绝大多数大中型网络在网络边界都有 Cisco 路由器，所以作者在本书中关注边界安全问题和如何使用 Cisco 路由器来处理这些问题。这不是一本用于认证的书，而是一本指导我们“如何做”的书。

本书采用以下方法来帮助我们完成“如何做”的过程：

- 提供解释和信息来补充我们的知识盲点；
- 解释各种 Cisco IOS 软件安全特性的优缺点，帮助我们理解什么时候应该使用它们；
- 使用来自作者个人咨询经验的小例子，来描述相关安全的问题；

- 提供很多例子，包括本书末尾的一个详细的案例学习，介绍如何实施 Cisco 的安全特性。

本书读者对象

本书打算为用作边界防火墙解决方案的 Cisco 路由器提供必要的体系结构。出于这个目的，这本书是一本有关“如何做”的书。虽然通过使用本书也可以完成其他目的，如准备 Cisco 的 CCSP SECUR 考试，但是写作本书的主要目的是：使用 Cisco 路由器来保护边界网络的安全。

本书假定读者对 Cisco 路由器、Cisco IOS 软件操作系统和命令行界面（Command-Line Interface，CLI）有基本的了解。假定读者有中到高级的 Cisco 路由器知识，读者至少应该持有 Cisco 的 CCNA 证书，这样才能理解和更好地使用本书中的内容。

因为本书关注使用 Cisco IOS 软件来增强边界路由器的安全，所以本书对当前必须保护网络边界安全的网络管理员和工程师，以及需要增强网络中其他路由器安全的任何人都非常有用。

本书的组织结构

虽然可以逐章阅读本书，但读者也可以有选择性地阅读某些章节，只学习感兴趣的内容。但是，每部分和每部分中的每章都是建立在之前的内容之上的。本书共分为 9 个部分。每个部分讲述边界路由器安全的一个重要组件，每一章介绍用 Cisco IOS 软件特性来实施边界路由器的安全。本书各章包括下面这些主题。

- **第一部分，“安全概述和防火墙”**
  - **第 1 章，“安全威胁”**——本章简要地概述了在保护网络时会面临的各种威胁，以及用来处理这些威胁的基本解决方案。本章一开始讨论安全问题的起因。然后对安全威胁进行了分类，列出了一些我们会面临的常见和不是很常见的安全威胁：它们是如何实施的，并概述了如何处理它们。本章为本书的其余部分奠定了基础。本章主要关注防火墙技术来保护网络边界。
  - **第 2 章，“防火墙概述”**——本章概述了防火墙技术和各种不同的防火墙实现。首先简要介绍了 OSI 参考模型，然后使用该模型来解释各种不同类型的防火墙技术如何提供不同级别的保护。本章也概述了防火墙的设计，包括通常用来提供防火墙解决方案的组件。最后，本章对本书中讨论的各种技术作了简介。
- **第二部分，“管理到路由器的访问”**
  - **第 3 章，“访问路由器”**——本章是本书中讨论 Cisco IOS 软件特性及其实施的第一章。第 3～5 章讨论如何使用 Cisco IOS 软件特性来保护到路由器自身的访问。本章关注到边界路由器的安全的基本访问。本章讨论各种不同的访问路由器的方法，以及可以用来保护这些访问类型的解决方案；本章也提供了有关使用某些类型访问方法的警告。另外，本章讨论了如何设置边界路由器上的不

同级别的 EXEC 访问，以及如何为账户指定不同级别的访问。

— **第 4 章，“关闭不必要的服务”**——本章介绍如何关闭全局服务，如何关闭接口服务，以及如何使用 AutoSecure 特征。AutoSecure 是 Cisco IOS 软件的一个新特性，类似系统配置对话脚本，可用来自动实施路由器基本安全。

— **第 5 章，“认证、授权和记账”**——本章讨论使用 AAA 来保护边界路由器。AAA 有很多特性，但本章只关注保护边界路由器安全的特性，包括本地和远程 AAA 的用法。

- **第三部分，“无状态的过滤技术”**
  - — **第 6 章，“访问列表概述”**——本章概述访问控制列表（Access Control List，ACL）。如果读者持有 CCNA 证书，应该对这些内容比较熟悉。
  - — **第 7 章，“基本访问列表”**——本章包括以下类型的基本 ACL：编号的、命名的、标准的、扩展的和定时的 ACL。本章也讨论一些新的 ACL 特性，如有序的 ACL（具有在已有列表中的任何位置删除任何 ACL 条目或插入新的 ACL 条目的功能）、ACL 注释、ACL 信息的日志记录和 turbo ACL（编译 ACL 来改进路由器的处理效率）。本章的最后部分关注使用 ACL 来阻塞各种类型的安全威胁和攻击，如欺骗、DoS、特洛伊木马和蠕虫攻击，以及不必要的或有害的服务，如端到端（Peer-to-Peer，P2P）的文件共享和即时消息（Instant Messenger，IM）程序。
- **第四部分，“有状态的和高级的过滤技术”**
  - — **第 8 章，“反射访问列表”**——本章讨论反射 ACL（Reflexive ACL，RACL）的用法。RACL 是 Cisco 的 CBAC 技术的先驱，这是一个半有状态防火墙特征。本章还讨论使用 RACL 来为边界路由器实施有状态防火墙功能的优缺点。本章最后给出了一个在两接口和三接口的边界路由器上使用 RACL 的例子。
  - — **第 9 章，“基于上下文的访问控制”**——本章介绍 Cisco 推荐使用的有状态防火墙特征：CBAC。因为这是介绍 Cisco IOS 软件防火墙特征集的第一章，所以首先简要介绍了这些特征。接着讨论了 CBAC 的优点和局限性，然后讨论它的实施。CBAC 的一些组件，如 DoS 保护，将在后面的章节中介绍。本章最后给出了几个例子，包括一个复杂的三接口路由器的例子。
  - — **第 10 章，“过滤 Web 和应用流量”**——本章介绍对应用层流量的过滤，包括 Web 流量。本章的开始部分介绍 Web 流量过滤，包括对 Java 小程序和嵌入在 HTTP 请求中的 URL 的过滤。本章的后半部分介绍基于网络的应用识别（Network-Based Application Recognition，NBAR）特性。NBAR 一般用来在路由器上实施 QoS 功能；然而，它也可以用来实施带宽和安全策略。本书的其他地方也讨论了 NBAR 的使用，这是一个很有用和很灵活的 Cisco IOS 软件特性。
- **第五部分，“地址转换和防火墙”**
  - — **第 11 章，“地址转换”**——本章介绍路由器上的地址转换功能。本章一开始概述了什么是地址转换、转换的各种类型和它们的局限性。本章的后半部分讨论这些类型的地址转换的实施。
  - — **第 12 章，“地址转换问题”**——本章关注一些地址转换带来的关键问题和处理这些问题的解决方案。首先讨论嵌入地址的问题，以及在地址转换时 Cisco IOS

软件如何处理这些问题。然后介绍使用地址转换时如何集成冗余功能，尤其是对于那些执行地址转换的设备。另外，本章还讨论负载平衡的各种方法，如热备份路由选择协议（Hot Standby Router Protocol，HSRP）和服务器负载平衡（Server Load Balance，SLB）。

- **第六部分，“管理通过路由器的访问”**
  - **第 13 章，“锁和密钥访问列表”**——本章介绍锁和密钥 ACL 的用法，以便在授予通过路由器的访问权之前首先认证用户连接。这是 Cisco 针对这个问题开发的第一个解决方案，起初打算用于拨号访问；然而，它也可以用来认证通过边界路由器传输流量的用户。
  - **第 14 章，“认证代理”**——本章介绍另一个 Cisco IOS 防火墙特征集的用法：认证代理（Authentication Proxy，AP）。AP 是 Cisco 推荐使用的特征，该特征用于在允许通过路由器传输流量之前首先认证用户。本章介绍了和锁和密钥 ACL 相比，AP 所拥有的很多优点，以及它的实施。
  - **第 15 章，“路由选择协议保护”**——本章讨论在路由器上对路由选择过程的保护，这反过来控制路由器的数据流。本章关注路由选择协议的认证，以及如何保护路由器免受路由选择和欺骗攻击。这些概念包括黑洞路由、内部网关协议（Interior Gateway Protocol，IGP）安全、BGP 安全和逆向路径转发（Reverse-Path Forwarding，RPF）。
- **第七部分，“检测和阻止攻击”**
  - **第 16 章，“入侵检测系统”**——另一个 Cisco IOS 软件防火墙特征集的组件是带有基本 IDS 组件的检测攻击特征。本章首先介绍了 IDS，包括签名，然后介绍边界路由器上 IDS 的配置。
  - **第 17 章，“DoS 防护”**——本章介绍保护路由器和网络免受 DoS 攻击的解决方案。本章的开始部分讨论如何检测 DoS 攻击；后半部分讨论可用来防护 DoS 攻击的工具，包括 TCP 截取、CBAC 和速率限制。
  - **第 18 章，“记录日志事件”**——本章讨论如何在边界路由器上设置日志记录。本章介绍基本的日志记录，以及使用系统日志将日志记录到外部服务器。本章也介绍将时戳用于日志记录以及在路由器上定义时间选项，包括手动和使用网络时间协议（Network Time Protocol，NTP）来实现。嵌入式系统日志管理器（Embedded Syslog Manager，ESM）一节讨论如何定制 Cisco IOS 软件的系统日志功能，包括 E-mail 告警。本章的最后部分简要讨论了应该查找日志文件中某些种类的信息来找到对路由器和网络的攻击。
- **第八部分，“虚拟专用网”**
  - **第 19 章，“站到站的 IPSec 连接”**——本章讨论使用边界路由器来终结站到站的 IPSec 连接。本章一开始讨论准备需求，然后继续讨论 IKE 阶段 1 中的管理连接的配置，包括设备认证选项。后半部分介绍 IKE 阶段 2 中的数据连接的设置，包括 IPSec 连接的排错。
  - **第 20 章，“远程接入 IPSec 连接”**——本章讨论使用边界路由器来终结远程接入 IPSec 连接。本章一开始概述远程接入，包括如何建立远程接入连接。本章的其余部分讨论使用 Easy VPN 特征来建立远程接入连接。

- **第九部分，“案例学习”**
  - **第 21 章，“案例学习”**——本章包括一个案例学习和全书中讨论的很多特性的实施。本章为保护边界网络给出了一个解决方案，并针对一家公司的问题作出解释。

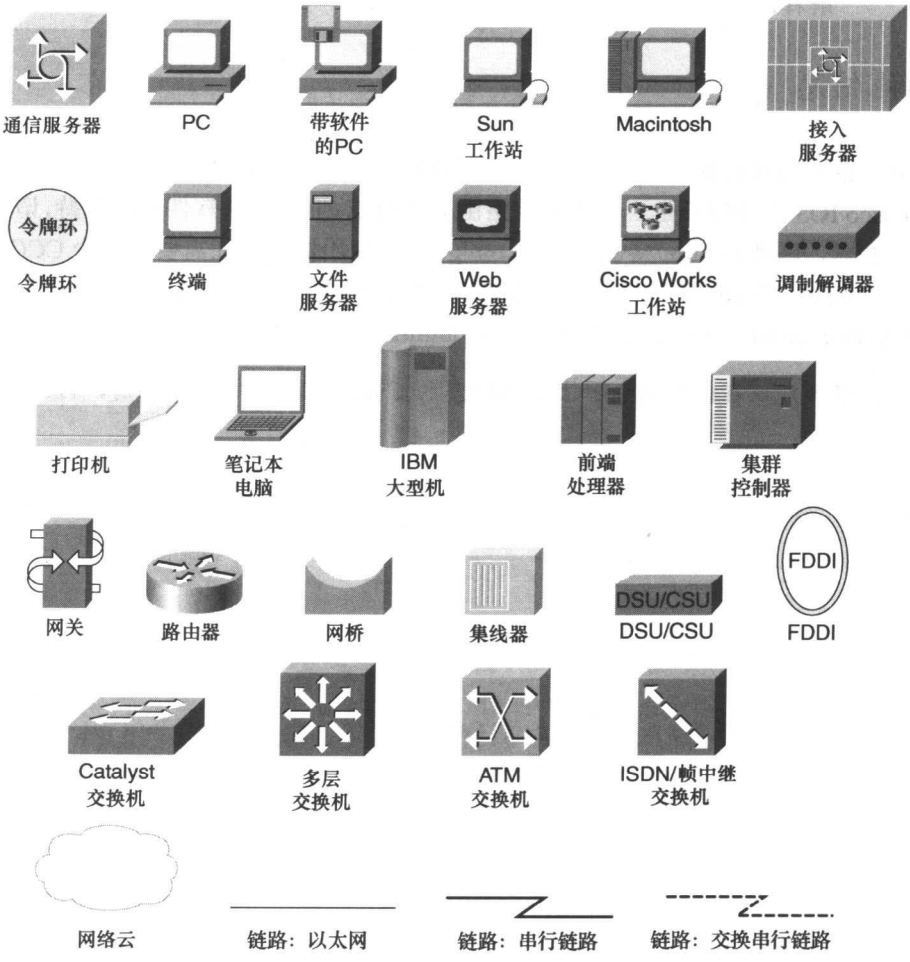
其他信息

本书讨论的很多特征只在几种不同的路由器型号或 Cisco IOS 软件版本中被支持。要了解一个 Cisco IOS 软件特征是否被特定的路由器平台或 Cisco IOS 软件版本支持，请使用 Cisco 的特征导航器，网址是 http://www.cisco.com/go/fn。使用这个特征需要有一个 CCO 账号。

要获得相关 Cisco 产品和 Cisco IOS 软件版本的产品安全建议和布告列表，请访问 http://www.cisco.com/warp/public/707/advisory.html。

提示：强烈建议在边界路由器上加载特定的 Cisco IOS 软件版本之前，仔细地查看这个列表。

本书使用的图标



命令语法约定

本书用来表示命令语法的约定和 Cisco IOS 命令参考中使用的约定是相同的。这些命令参考对这些约定作了如下描述：

- **黑体字**指示字面显示的命令和关键字。在实际的配置例子和输出（并非一般的命令语法）中，黑体字指示由用户手工输入的命令（例如 **show** 命令）；
- *斜体字* 指示需要提供实际值的参数；
- 竖线（|）分隔替换项，相互排斥的元素；
- 方括号（[ ]）指示可选元素；
- 大括号（{ }）指示必需的选项；
- 方括号内的大括号（[{ }]）指示在一个可选元素中必需的选项。

目　录

第一部分　安全概述和防火墙

第三部分 无状态的过滤技术

第四部分 有状态的和高级的过滤技术