组网用网丛书

网络安全
Cisco 解决方案

Cisco Secure Internet Security Solutions

[美] Andrew G. Mason
Mark J. Newcomb 著

詹文军 等译

CISCO SYSTEMS
CISCO PRESS

PHEI

電子工業出版社
Publishing House of Electronics Industry
www.phei.com.cn

网络安全 Cisco 解决方案

Cisco Secure Internet Security Solutions

[美] Andrew G. Mason
Mark J. Newcomb 著

詹文军 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

虽然Cisco Systems公司通过推出Cisco Secure产品系列来帮助客户建立安全的网络，但到目前为止，国内尚没有使用Cisco Secure产品系列来解决因特网安全性问题的出版物，本书的出版填补了这一空白。本书英文原版的作者都是具有高深资历的网络安全专家，其中主笔人Andrew G. Mason作为一位Cisco网络认证工程师，具有多年使用Cisco Secure产品来设计和实现网络安全解决方案的丰富经验，为本书内容的权威性提供了充分的保证。本书内容覆盖了因特网安全性基础，并对Cisco Secure产品系列中的每种产品进行了集中介绍，提供了因特网安全所需要的优选配置示例。

本书主要针对网络工程师和网络设计人员，其基本读者是负责企业网连接或Cisco Secure产品安装的网络工程师和设计人员，也适用于负责网络安全以及对Cisco Secure产品感兴趣的其他网络人员、参加CCIE和CCDP/CCNP认证考试的人员、业界专家等。

图书在版编目（CIP）数据

网络安全Cisco解决方案/（美）梅森（Mason, A. G.）著；詹文军等译. —北京：电子工业出版社，2002.1
书名原文：Cisco Secure Internet Security Solutions
ISBN 7-5053-7292-0

Ⅰ.网… Ⅱ.①梅…②詹… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2001）第088110号

书　　名：**网络安全Cisco解决方案**
原 书 名：Cisco Secure Internet Security Solutions
著　　者：[美] Andrew G. Mason　Mark J. Newcomb
译　　者：詹文军 等
责任编辑：谭海平　窦　昊
排版制作：今日电子公司制作部
印 刷 者：北京东光印刷厂
出版发行：电子工业出版社　www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：23.5　字数：601.6千字
版　　次：2002年1月第1版　　2002年1月第1次印刷
书　　号：ISBN 7-5053-7292-0 / TP·4182
定　　价：35.00元
著作权合同登记号　图字：01-2001-1439

译 者 序

Cisco Systems公司通过推出Cisco Secure产品系列致力于帮助其客户来建立安全的网络，但到目前为止，国内尚没有使用Cisco Secure产品系列来解决因特网安全性问题的出版物，本书的出版填补了这一空白，本书英文版的作者都是具有高深资历的网络安全性专家，其中主笔人Andrew G. Mason作为一位CCIE，其多年来使用Cisco Secure产品来设计和实现网络安全性解决方案的丰富经验为本书内容的权威性提供了充分的保证。

作为译者，我们希望能够尽自己的最大努力将这一本好书忠实、完整、正确地译出，希望它既能够符合国人阅读习惯，又能保证其原汁原味，如果能够达到这一目的，我们就觉得很欣慰了。

参加本书翻译的有：詹文军、廖铮、卢陈思、索为群、黄国平、孙大庆、白常青、张伟、张建伟、林依然、高博、吉明宇、黎建辉、姜楠、候捷、钱林海、李波等人，由詹文军负责统稿。

最后希望热心的读者对本书中的各种错误进行指正，谢谢。

前　言

因特网对于许多大企业来说已成为核心的业务驱动器，但是，随着业务的发展，安全性问题随之而来。最近的许多新闻头条常常出现关于大型电子商务站点被黑，造成潜在的灾难性后果的文章。

Cisco Systems公司致力于帮助客户通过网络安全性设计建立安全的网络连接，在这些网络安全性设计中，Cisco Secure产品系列扮演了重要的角色。目前还没有关于使用Cisco Secure产品系列来处理因特网安全性的公开出版物，出版本书的目的正是在于此。本书的内容覆盖了因特网安全性基础，并对Cisco Secure产品系列中的每种产品进行了集中介绍，提供了丰富的解释以及为因特网连接提供安全性所需要的优选配置示例。

本书首先开始介绍由因特网所带来的安全性威胁，然后对Cisco Secure产品系列进行了完整的解释，同时对该产品系列中的每种产品进行了详细的讨论，而且还对如何根据具体环境的需求来对每个单独的组件进行配置提出了建议。另外，本书对Cisco Secure PIX防火墙进行了深入的介绍，从提出一个体系结构化的观点，到提供一个有关常用PIX命令和它们实际应用的参考。虽然本书关注的是因特网安全性，但它对于一般的网络安全性也是可用的。

读者对象

本书针对网络工程师和网络设计人员。其基本读者是负责企业网连接或Cisco Secure产品安装的网络工程师和设计人员。其他的一些读者则可以是对和他们所在的特定企业网环境相关的网络安全性和Cisco Secure产品感兴趣的其他网络人员。

另外，有志于通过CCIE和CCDP/CCNP认证的那些人可以在本书中获得提高其因特网安全性水平的内容。

本书面向中级和高级读者，由于本书内容的惟一性，一些业界的专家也可将本书作为参考。

读者阅读本书应具备的条件

本书中的内容假定读者已经熟悉了一般的网络概念和术语，其中包括对TCP/IP网络协议的完整了解，或者是已经熟悉了由电子工业出版社出版的《网络互联技术手册（第三版）》和《IP路由基础》中的内容。

覆盖的内容

本书分为11章和一个附录：

- 第1章提供了对因特网的一个历史回顾，以及和因特网有关的风险。
- 第2章介绍了Cisco路由器和相关的安全性威胁，以及从因特网的角度来看，这些路由器所具有的安全性弱点。另外还提供了示例配置来作为用户实现自己的企业因特网路由

器的参考。

- 第3章提供了Cisco安全性解决方案和Cisco Secure产品系列。下面的6章对每种产品进行了详细的介绍。
- 第4章介绍了Cisco Secure PIX防火墙，并提供了对PIX的一个技术性概述，以及根据一个案例研究来提供的一个配置指导和示例配置。
- 第5章介绍了Cisco IOS防火墙，并提供了示例配置，而且对其中的主要技术进行了解释说明。
- 第6章介绍了一种最新出现的安全性技术，入侵检测。本章对各种入侵检测系统的类型进行解释，然后针对网络边界入侵的情况，提供了分别针对Cisco路由器和Cisco Secure PIX防火墙的示例配置。
- 第7章内容覆盖了Cisco Secure Scanner，并对网络扫描和其正当和非法的使用进行了简短的说明，然后深入介绍了Cisco所提供的Cisco Secure Scanner产品。
- 第8章介绍了Cisco Secure Policy Manager（CSPM），CSPM提供了一个针对企业网的集中化管理平台，该企业网中包含了运行Cisco IOS防火墙软件的Cisco路由器和Cisco Secure PIX防火墙。另外，本章提供了一个CSPM的示例安装和配置过程。
- 第9章介绍了Cisco Secure访问控制服务器（ACS）和它在网络中的使用。另外本章还提供了分别针对网络访问服务器（NAS）和Cisco Secure ACS服务器部分的配置。
- 第10章介绍了一个常见的企业网络，并列举出和外部连接相关的安全性威胁。另外还提供了对付安全性风险的各种提示和配置解决方案。
- 第11章集中介绍了因特网服务和能够为它们提供的安全性保护。本章的内容以这些公共服务器位于ISP或企业网DMZ作为基础，对每种因特网服务进行了介绍，并说明了各自潜在的安全性风险和减轻这些威胁的方法。
- 附录A“Cisco SAFE：针对企业网的安全性蓝图”——SAFE作为Cisco针对企业网的一个安全性蓝图，它的基本目标是为那些感兴趣的团体或个人提供有关设计和实现一个安全的网络的最佳实践信息。SAFE可以作为网络设计人员在考虑网络中安全性需求时所参考的一个指导手册。另外，SAFE采用了一种defense-in-depth（深入防范）的方式来进行网络安全性设计，这种类型的设计将视点聚焦于所预期的威胁以及减轻这些威胁的方法，而不是“在此放置一个防火墙，在那放置一个入侵检测系统”这种浅泛的指导。这种策略使网络的安全性采用了分层设计设施的方式，使得某个安全性系统的失效不太可能导致网络资源遭到损害。另外，SAFE基于Cisco公司和其合作伙伴所生产的产品。

语法约定与图标

在本书中的命令语法遵循以下约定：

- 命令、关键字和实际的参数值以粗体显示。
- 参数（需要提供实际的值）以斜体显示。
- 可选关键字或参数（或者是可选关键字或参数的选项）位于中括号[]中。
- 必须具有的关键字或参数位于大括号{}中。

注意：以上约定只针对命令语法，实际的配置和示例不遵循这些约定。

下图列举了本书中使用的大多数重要设备的图标。

目　录

第一部分　因特网安全性基础

第二部分 Cisco Secure 产品系列

第三部分 因特网安全性环境

第四部分 附 录

第一部分
因特网安全性基础

第1章　因特网安全性

本章包含以下内容：

- 因特网威胁
- 网络服务
- TCP/IP 协议集的安全性
- 拒绝服务攻击
- 创建企业安全性策略
- 小结
- 常见问题
- 词汇表

本章介绍网络安全性的一些基础内容，首先对最常见的攻击形式进行一番简介，然后介绍一些网络设备类型的特性。

Cisco Secure IOS 软件专门设计为用于防止外界攻击对用户网络的影响，Cisco Secure 软件对未授权访问、拒绝服务（Dos，Denial of Service）攻击、人在中间（man-in-the-middle）攻击和许多其他常见的攻击方法可提供最高级别的防护，这些攻击方法或者是用来拒绝服务，或者是用于获得未授权信息。Cisco Secure IOS的安全性特性依赖于一些配置、硬件解决方案和技术，包括自适应安全性算法（ASA，Adaptive Security Algorithm），这些为当今的网络管理员提供了最佳的网络安全性。

随着技术的发展，Cisco公司也一直不断地改进其硬件和软件安全性解决方案以维持其在网络安全性领域的先进性。本书对一些通过 Cisco Secure 解决方案的使用可提供的网络安全防护方法进行了探讨。

为介绍防止网络攻击的基本内容，本章的内容覆盖了一些协议，包括传输控制协议（TCP）、网际协议（IP）、地址解析协议（ARP）和用户数据报协议（UDP）等协议的格式，同时还介绍了最常见的 DoS 攻击形式。在本章以后的章节中提供了一些用于对付 DoS 攻击的专门技术。

本章的结尾则总结了企业安全性策略的需求和使用。

1.1　因特网上的威胁

因特网是由专用主机和公共主机所组成的一个集合。事实上，任何拥有一台计算机的人都可以通过某种方式连接到因特网，在任何时候，因特网上都存在着成百上千个个体。虽然这些个体中的大多数都没有不良企图，但总是有一些人，因为各种原因，试图渗透或摧毁位于网络上的服务。有时候网络会被这样一种技术所攻击，在这种技术中，无辜的第三方被利用来发起攻击。例如，一个系统被某种蠕虫病毒所感染的个体会非有意地将这一蠕虫病毒传递给所有和