NETWORK PROFESSIONAL'S LIBRARY

本书涵盖：风险评估、隐私问题、黑客技术，等等

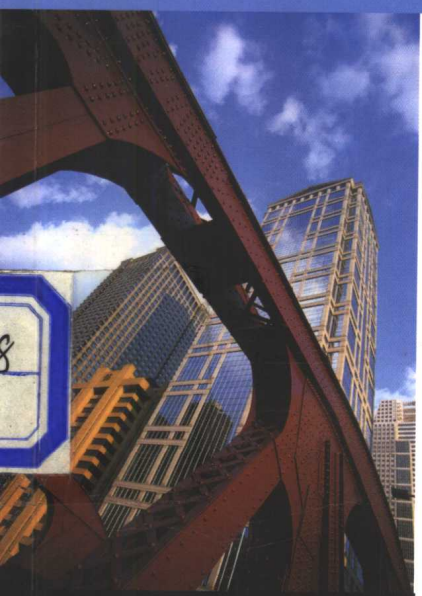
“有些网络和系统管理员发现，他们自己不但要负责整个网络的运行，而且还要维护网络的安全，对于这些人而言，这确实是一本适合他们的好书。书中精心划分的章节和浅显易懂的内容令读者对所有最新的安全技术清晰明了，这些技术从基础知识发展而来并建立在那些概念之上。”

—— Mike Schiffman
Guardent公司研发部主管

Network Security
A Beginner's Guide

网络安全实用指南

[美] Eric Maiwald 著
天宏工作室 译



- 建立和维护一个安全的网络
- 使用防火墙、防病毒软件、入侵检测系统等安全技术
- 连接到Internet并安全地从事电子商务交易
- 8页蓝图中给出了网络设计的示例

OSBORNE
计算机专业技术丛书

清华大学出版社

Osborne 计算机专业技术丛书

网络安全实用指南

[美] Eric Maiwald 著

天宏工作室 译

清华大学出版社

北京

网络安全实用指南
Eric Maiwald：**Network Security：A Beginner's Guide**
EISBN：0-07-213324-4

图书在版编目（CIP）数据

网络安全实用指南/（美）迈瓦尔德著；天宏工作室译. —北京：清华大学出版社，2002
（Osborne 计算机专业技术丛书）
书名原文：Network Security：A Beginner's Guide
ISBN 7-302-06197-1

Ⅰ. 网…　Ⅱ. ①迈… ②天…　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（2002）第 106241 号

出 版 者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.tsinghua.edu.cn
责任编辑：刘映欣
印 刷 者：世界知识印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　**印张**：23.75　**插页**：4　**字数**：489 千字
版　　次：2003 年 3 月第 1 版　2003 年 3 月第 1 次印刷
书　　号：ISBN 7-302-06197-1/TP・3704
印　　数：0001～4000
定　　价：46.00 元

出版说明

随着计算机技术的深入发展及最新网络操作系统的问世，越来越多的企业和个人逐渐将自己的注意力和兴趣转移到了网络技术上。有关网络的软硬件配置、网络协议、网络安全、网络数据库、网络应用程序开发（特别是Web应用程序开发）等方面的主题备受关注。计算机专业人士和广大计算机爱好者迫切需要一套可以从中汲取网络专业知识的权威书籍。为此，我社选择了美国Osborne/McGraw-Hill出版的Network Professional's Library、Professional Developer's Library和Database Professional's Library等专业性较强的图书，组织成这套Osborne计算机专业技术丛书。我们真诚地希望将这一套丛书作为信息时代的礼物奉献给广大读者。

本套丛书的特点是注重理论方法和实际应用的相互结合。在理论上，讲究技术的新颖和原理的深入；在应用上，讲究方法的直观性和广泛适用性。通过认真学习，读者可以充分地将自己已有的知识融入新技术的学习和掌握中，从更深的层次上理解目前不断出现的新概念、新技术，并且很容易在较短的时间内获得丰硕的学习成果，所有这一切都源于这些图书科学的编排结构、清晰的文字表达和富有代表性的应用示例。目前，计划出版和已出版的一系列图书已经获得广大读者的热切关注和强烈反响，我们坚信我社一贯奉行的打造精品图书的理念会为读者带来巨大的收益。

麦格劳-希尔教育出版集团拥有世界知名的计算机图书出版品牌——Osborne/McGraw-Hill，这是美国出版IT图书的独树一帜的力量。Osborne/McGraw-Hill具有针对普通用户和专业人士的多种图书系列，立足于编程（Programming）、联网（Networking）、数据库（Database）、认证（Certification）以及大众（Consumer）图书五大方向，每年出版图书250余种。由于与Oracle、Cisco、Corel、Global Knowledge和J.D. Edwards等国际著名企业建立了长期战略合作出版关系，Osborne一直拥有最前沿的IT技术图书。相对于其他计算机图书而言，Osborne的系列化图书产品和专业化IT技术参考书目更具特色。这些图书全部由富有技术经验和才华的计算机开发人员编写，将为第一线的专业人士提供最新、最准确和最富于创造性的计算机知识、理论及开发应用的经验。

天宏工作室负责本套丛书的翻译工作，在此感谢他们为此付出的辛勤劳动。

作者简介

Eric Maiwald，CISSP

Eric Maiwald 是 Fortrex Technologies 公司的 CTO（Chief Technology Officer），他负责检查公司的所有安全研究和培训活动。Maiwald 先生还执行评估工作、制订策略，并为大的金融机构、服务公司和制造商实现安全方案。作为一名顾问、安全负责人和开发人员，他在安全领域有着丰富的经验。他获得过 Rensselaer Polytechnic Institute 颁发的电子工程学专业的学士学位，获得过 Stevens Institute of Technology 颁发的电子工程学专业的硕士学位，并且是信息系统安全认证专家（CISSP）。他是以下专利的发明人：专利号为 5 577 209 的“为网络上的计算机和终端之间的通信提供多级别安全的设备和方法”；专利号为 5 872 847 的“使用信任联合在计算机网络中建立信任关系”。Maiwald 先生是许多知名安全会议的特邀嘉宾，他还是 SANS Windows Security Digest 杂志社的一位编辑。

技术评审员简介

Mark Cusick

Mark Cusick 目前是 Fortrex Technologies 公司（www.fortrex.com）安全服务部的主管。该公司位于马里兰州的 Gaithersburg，为客户提供信息安全解决方案。Mark Cusick直接负责 Fortrex Technologies 公司的所有安全服务活动。除了为大多数 Fortrex 客户开发策略和实现安全解决方案之外，他个人还参加了大量评估工作。

在加入 Fortrex Technologies 公司之前，Cusick 先生是美国军方在马里兰州 Ft. Meade 的 Technical Counterintelligence School 的主管。在此期间，他负责所有与高度敏感而复杂的国家级调研有关的培训和教育出版物的开发工作，其范围包括全世界大多数敏感设备的实际技术渗透和尝试进行的技术渗透。Cusick 先生指导开发了计算机安全和信息战领域的新课程。

Cusick 先生是美国军方的退休准尉，他在安全和信息安全领域拥有 30 多年的工作经验。

致谢

如果没有一些人的帮助，我是不会写出这本书的。其中最值得一提的是与我一起工作的人，Mark Cusick、Stephen Edwards、Bill Sieglein 以及 Lee Kelly，还有 Fortrex 的其他成员。还有两位人士提供了大量信息，他们是 Ted Whitehouse 和 Brian Ford，对此我非常感激。当然，如果没有 Osborne/McGraw-Hill 公司工作人员的帮助，那么这一切都是不可能的，最值得提及的是 Jane Brownlow、Ross Doll 和 LeeAnn Pickrell。

简介

《网络安全实用指南》一书的标题看上去已经将其内容定义得很清楚了。但是，本书不只是初学者的指南。在编写本书时，我每天都在设法对摆在我面前的问题作出选择。其中大多数问题在过去几年里曾让我感到手足无措，如果那时有这些信息在手边，那将对我产生很大的帮助。

最近几年，安全性越来越成为一个问题。我们总是能听到对 Web 站点和组织成功地进行了攻击的案例。为了对付这类事件，越来越多的厂商推出了可以提供某种保护的工具。通过对这类信息进行分析，可以得出的结论是：安全方面的大问题可以通过技术来解决。不幸的是，安全问题比这更复杂。在最底层，安全问题都是人的问题。无论我们在这方面投入了多少技术，我们能够做的最好的事情是让安全人员的工作更容易一些。我们不会使用技术解决基本问题，但是可以通过周密部署的安全过程和程序的具体应用来处理安全问题。希望本书能够为您提供用来处理安全问题的基本工具。

本书分为 4 个主要部分，在附录中还包含了一些有用的信息。

第一部分：信息安全的基础知识

第一部分为您提供了对什么是信息安全的基本概念的理解，从攻击和防御服务的角度定义了相应的术语。

▼ **第一章：什么是信息安全** 第一章提供了信息安全的基本定义。这是通过了解“保护的是什么”（信息）和“到底什么是安全性”来定义的。其中包括了安全性的历史，这是为了展示这一概念是如何随时间变化的，以及各种发展背后的思想。历史部分还会介绍过去那些失误是如何引导我们进入目前这种只有很少（或者根本没有）安全性的环境的。最后，这一章还指出了一些由不同厂商和团体导致的常见误区以及他们提供错误和误导信息的原因。

• **第二章：攻击类型** 第二章讨论攻击的基本形式以及每一种形式是如何对组织进行破坏的。这一章对每种攻击的基本形式进行了剖析，并提供了一些示例来展现攻击是如何进行的。

▲ **第三章：信息安全服务** 第三章讨论可以用来保护信息和系统不受攻击的基本安全服务。对每一种基本服务进行了分析，并提供了一些示例来展现这些服务是如何实现的。本章还介绍了每一种服务是如何对 4 种攻击进行防范的。

第二部分：基础工作

第二部分为您提供了安全计划的基础工作。要想开始一个计划，安全专家需要对法律、政策的运用方式、风险管理以及实现和管理安全的过程有一个了解。在这一部分的最后讨论了安全领域中的最佳实践。

▼ **第四章：信息安全的法律问题** 第四章介绍有关信息安全的法律问题。作为国家法律的例子，对现有的美国联邦法律进行了说明和讨论。同时对其他国家的法律进行了讨论，并与美国法律进行了对比。这里的关键是对犯罪行为的现有解释的区别。还简要讨论了责任问题，以表明在安全性方面还存在大量非刑事的法律问题。接下来的一部分介绍了隐私，这是Internet法律的一个新领域，对许多公司都有着潜在的影响。最后，本章重点讨论了当公司要起诉入侵者时应该采取的各种行动。

- **第五章：策略** 第五章讨论对策略的需要。在说明了策略的重要性之后，本章讨论各个组织应该制定的不同类型的策略。然后讨论如何制定合适的策略，以及在制定策略之后如何部署并有效地使用策略。
- **第六章：管理风险** 第六章的重点在于找出组织中的风险区域。本章的关键概念是将思路从威胁（入侵者）和薄弱环节（入侵者可以进入的地方）转移到风险（一旦攻击得手，对组织带来的后果）。首先定义了风险，然后说明识别风险的方法，最后讨论了如何管理风险。
- **第七章：信息安全过程** 第七章将所有基础工作合并在一起，说明了如何实现一个信息安全程序。过程的每一个阶段都从“如何去做”的角度进行讨论。

▲ **第八章：信息安全最佳实践** 第八章着重介绍“做哪些事情”（与第七章的“如何去做”相对应）。最佳实践是管理型安全措施与技术型安全措施的结合。本章定义了完美的安全计划。本章还讨论了完美的安全计划不存在的原因，以及计划趋近于完美的程度与组织的风险管理原则是紧密相关的。

第三部分：实际的解决方案

第三部分提供了有关结构、电子商务站点、加密以及入侵检测的详细技术信息。这一部分还提供了黑客寻找网络目标的方式以及用来攻击站点的特定技术的详细信息。

▼ **第九章：Internet 结构** 第九章详细讨论了与 Internet 的连接。本章讨论了

关键的结构问题、术语的含义以及每一部分如何用来保护从 Internet 到一个组织的连接。

- **第十章：虚拟专用网络** 第十章讨论虚拟专用网络（Virtual Private Network，VPN）的使用及其安装和管理。
- **第十一章：电子商务安全需求** 第十一章讨论了安装电子商务站点所涉及的问题。本章讨论电子商务项目的每一个领域，并指出每一领域中可能导致安全漏洞的问题。对于提出的每一个问题，都给出了可能的解决方案。
- **第十二章：加密** 第十二章提供了有关加密的信息，介绍了如何使用它来增强安全性。首先定义了基本的加密概念，然后给出了私钥和公钥系统的基本概念。其中包括了实际的示例以及对最流行算法的讨论。本章也介绍了数字签名的作用以及如何提供数字签名。在本章末尾包含了密钥管理和信任问题，并总结了有关加密使用问题的基本理解。
- **第十三章：黑客技术** 第十三章展示了大多数黑客试图对 Internet 站点采取的攻击类型。本章讨论了黑客的动机，并从两个角度——偶发性黑客寻找任何系统，专业黑客寻找特定组织——分析了黑客威胁。
- **第十四章：入侵检测** 第十四章提供了正确使用入侵检测系统以及入侵检测系统的作用的信息。本章讨论了 IDS 的最新技术、不同的 IDS 类型以及这些类型用于加强组织安全性的方式。本章的关键在于 IDS 系统不是万能药，需要大量资源才能有效地发挥作用。

第四部分：特定平台的实现

第四部分主要为常用操作系统提供具体的配置建议。这一部分给出了加强 Windows NT、Unix 和 Windows 2000 安全性的详细内容。

▼ **第十五章：Unix 的安全问题** 第十五章介绍了配置和管理 Unix 系统时所遇到的基本安全问题。

- **第十六章：Windows NT 的安全问题** 第十六章介绍了配置和管理 Windows NT 系统时遇到的基本安全问题。

▲ **第十七章：Windows 2000 的安全问题** 第十七章指出配置和管理 Windows 2000 系统时遇到的基本安全问题。

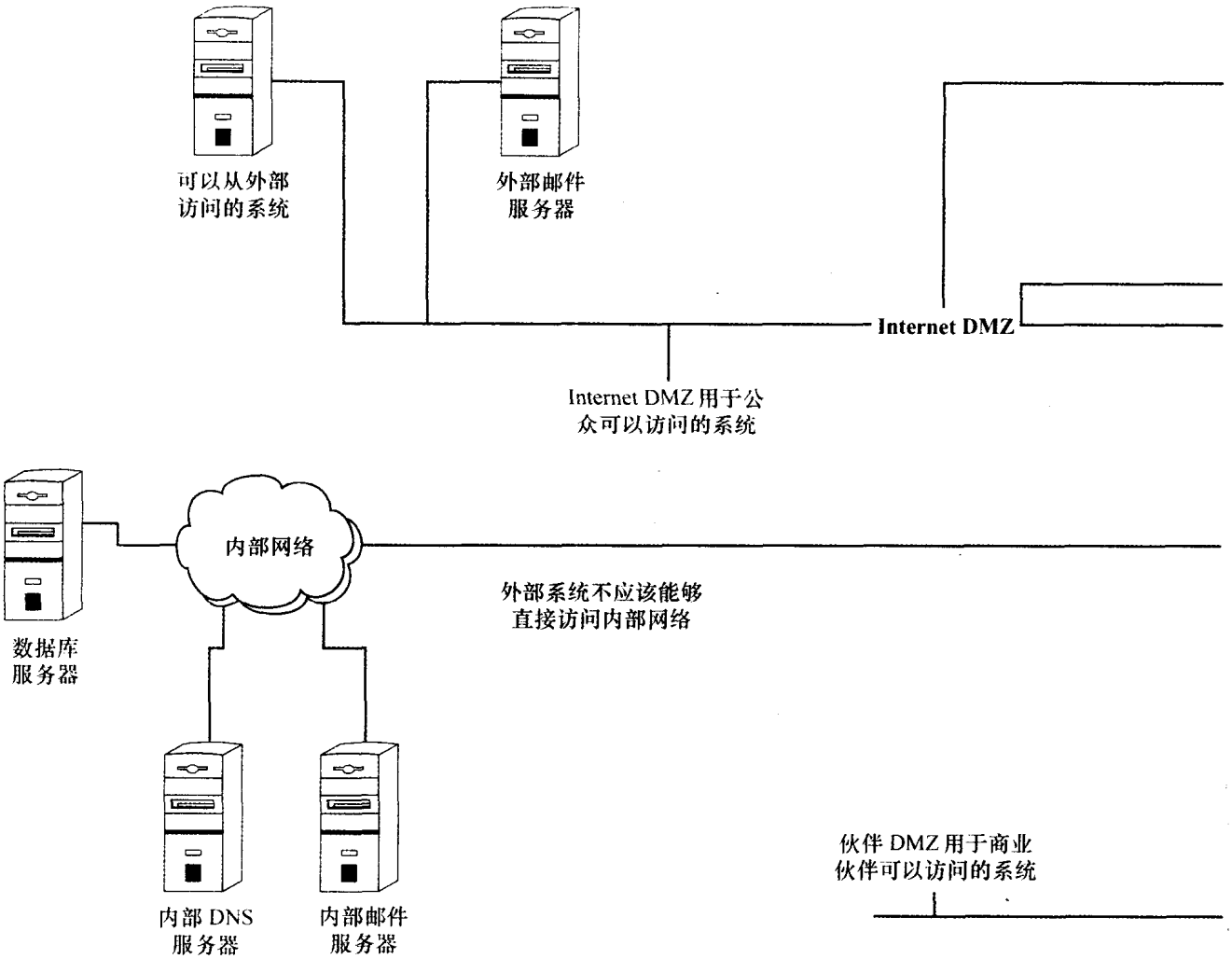
第五部分：附录

第五部分提供了 4 个对本书内容进行补充的附录。这些附录内容用于帮助读者解答有关安全性和实现一个强健程序的特定问题。

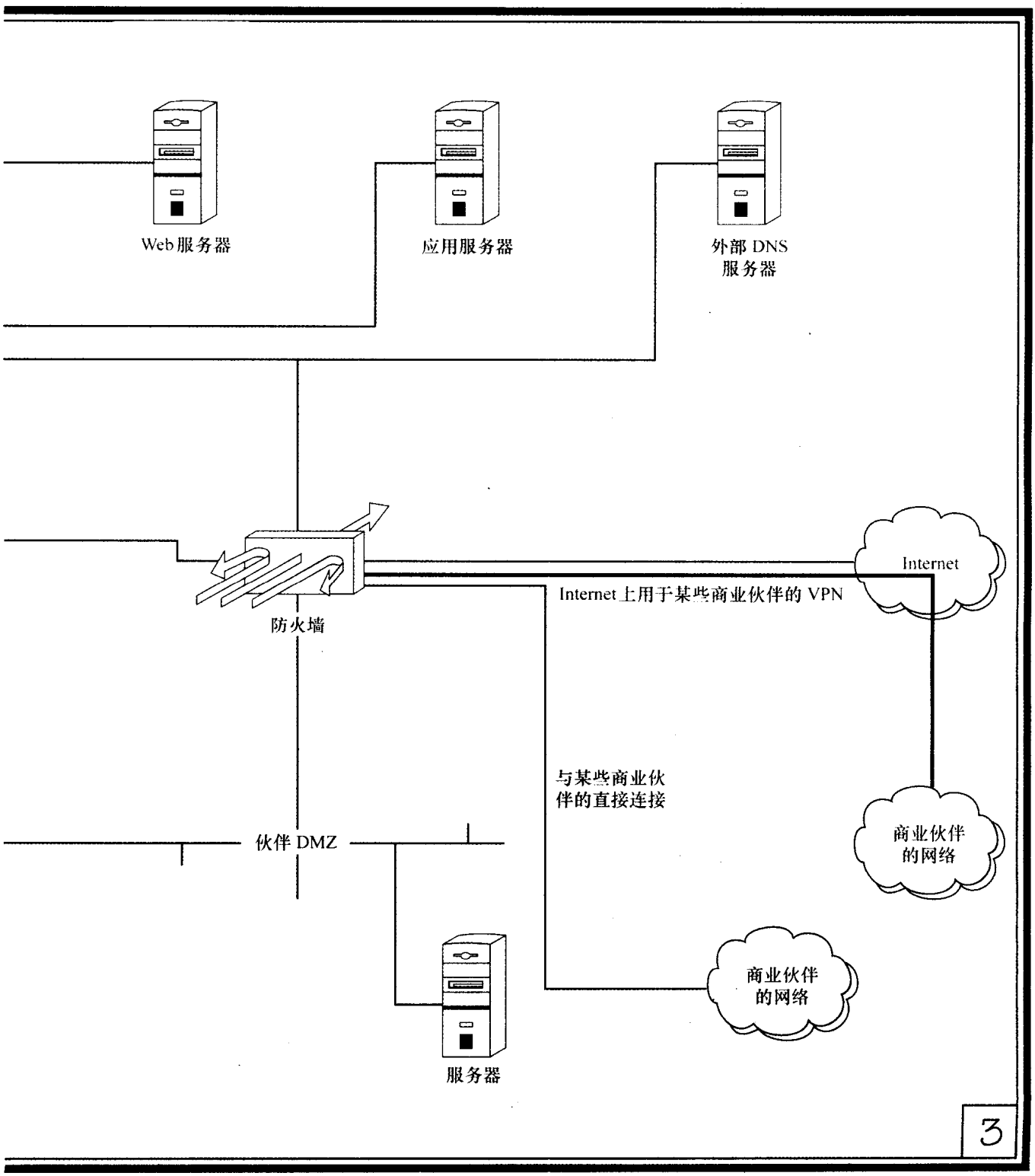
- ▼ **附录 A：进程项目计划** 附录 A 从不同的角度介绍了信息安全过程。在实际中，需要将进程转换为可行的项目计划，其中不同的任务可能会同时执行。该附录从这一角度对进程进行了分析。
- • **附录 B：Unix 与 Windows：哪一个更安全** 附录 B 对这个问题作了一些分析。看上去争论的双方都有自己的理由，通常要求安全人员作出最终判断。
- • **附录 C：可以学习更多安全性知识的资源** 附录 C 提供了举办安全会议的组织名称及联络信息。在这些会议中，对安全问题感兴趣的人可以了解更多的专业知识并且能够提高自身的技术级别。
- ▲ **附录 D：应急响应过程测试方案** 附录 D 提供了 10 个用于测试应急响应过程的方案（以及一些变化形式）。

总之，本书试图正确地介绍信息安全。我经常看到一些组织为了解决他们的安全问题而购买最新的安全工具，但是并没有认识到对安全管理人员进行良好培训并使员工了解安全的重要性是更加关键的。希望您将会发现本书中的信息是非常有用的。

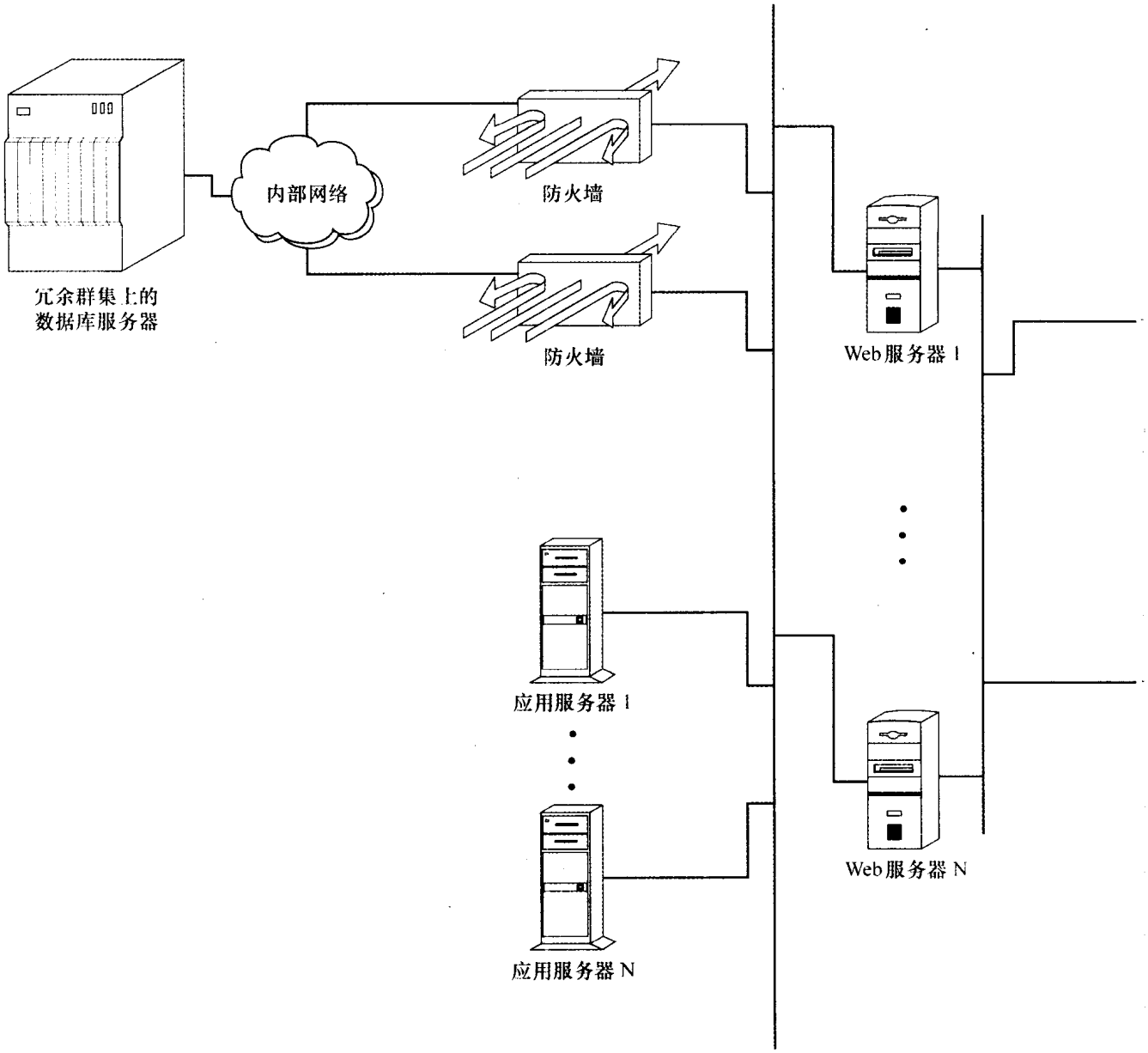
正确的 Internet 结构



2 组织的 Internet结构可以像需要的那样强健，以便满足组织的需求。不过，某些类型的安全机制应该将组织的内部网络从 Internet DMZ、伙伴 DMZ（如果有）以及 Internet 中分离出来。

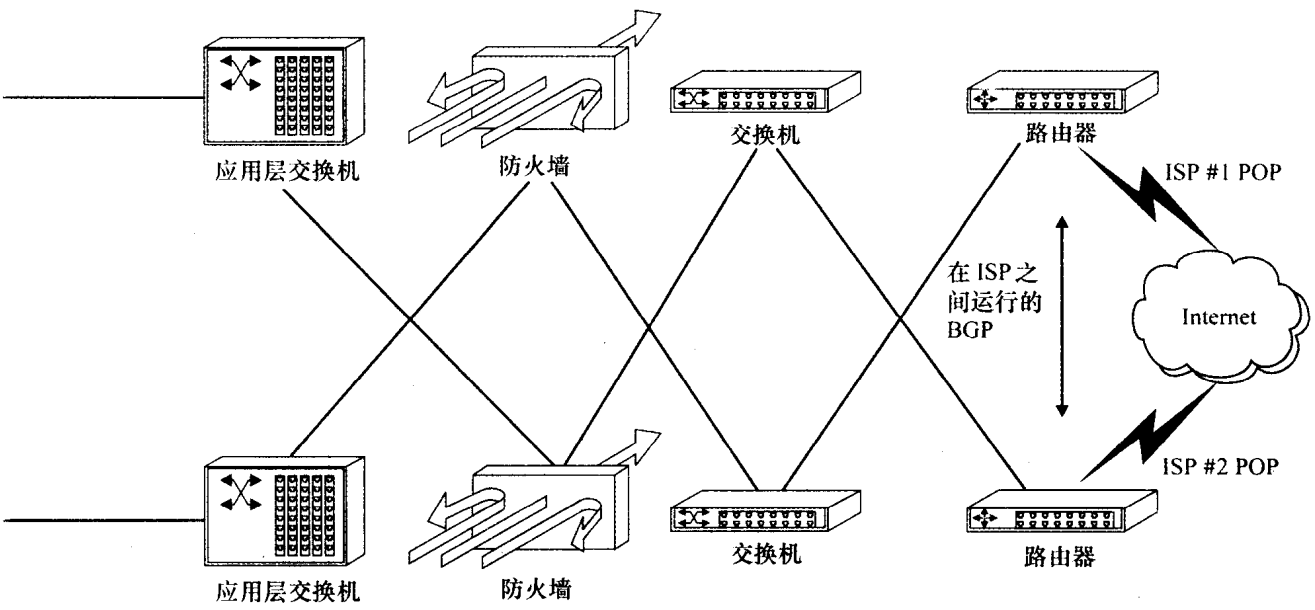

Web服务器
应用服务器
外部 DNS
服务器
防火墙
Internet
Internet上用于某些商业伙伴的 VPN
与某些商业伙
伴的直接连接
伙伴 DMZ
商业伙伴
的网络
商业伙伴
的网络
服务器

电子商务结构



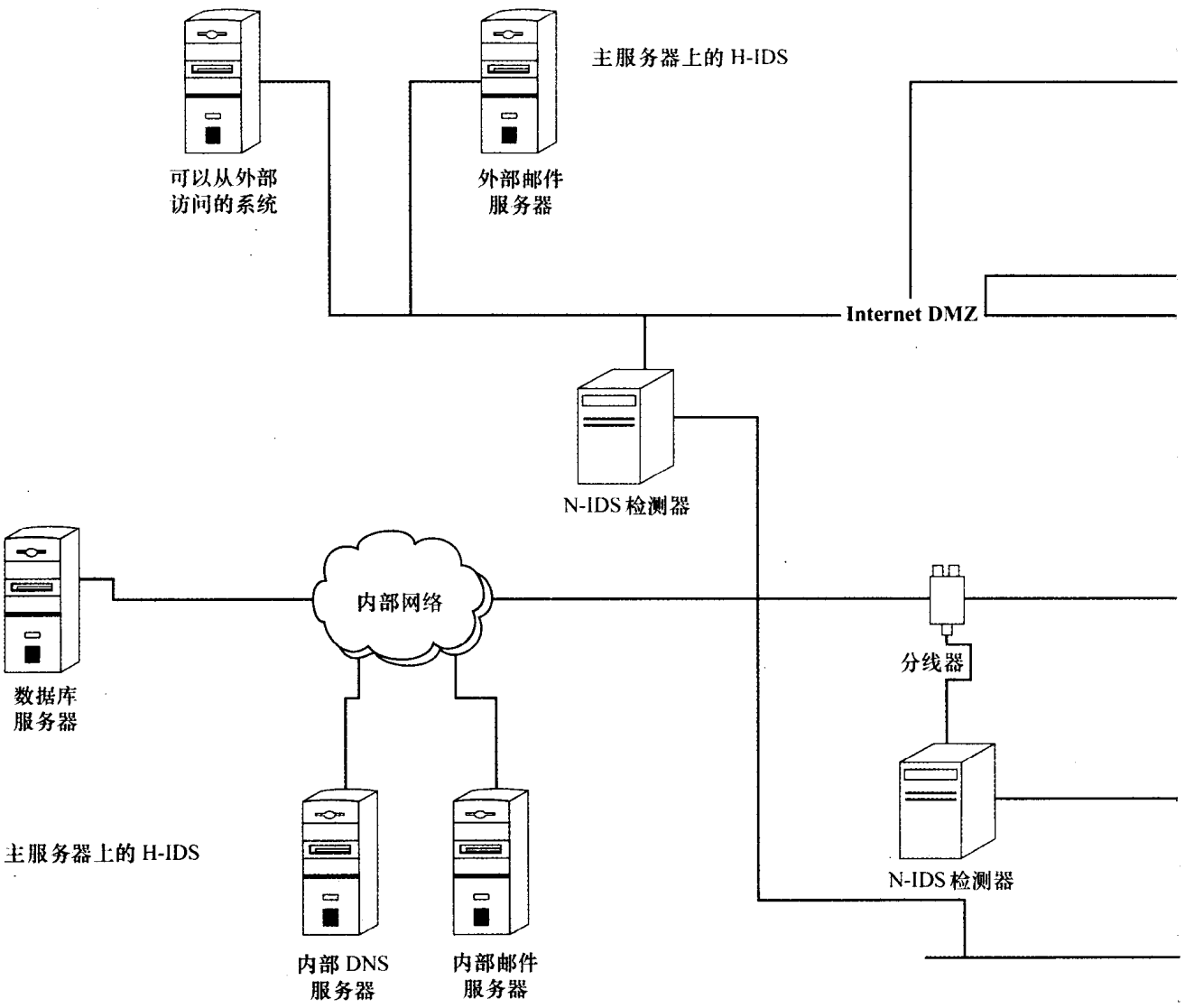
应用层交换机在 Web 服务器上提供了负载共享和故障转移

路由器和防火墙交叉连接到交换机上，以便提供冗余路径

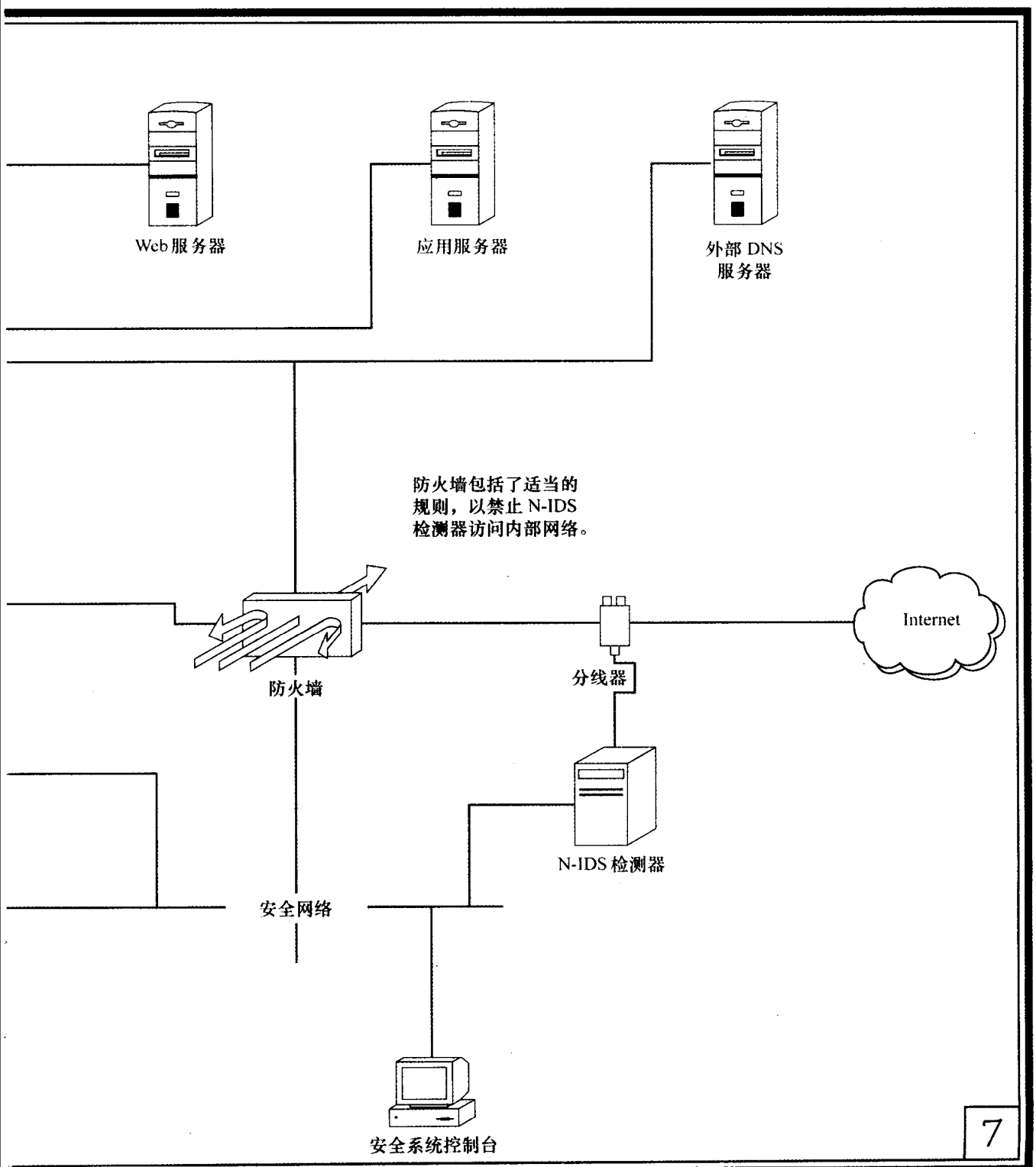


设计一个强健的电子商务结构依赖于许多网络组件正确地协调工作。这个结构所提供的主要安全服务是可用性。每一个组件都拥有冗余和故障转移。一台计算机的故障不会导致这个站点停止工作。

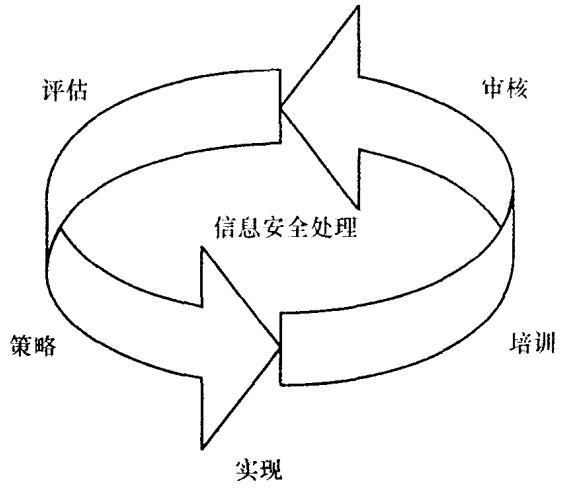
入侵检测系统结构



入侵检测系统的部署需要在通信结构以及策略创建方面非常小心。可以在主服务器上使用基于主机的 IDS。主服务器包括那些可以直接从 Internet 访问的服务器以及包含敏感信息的服务器。应该在通信基础机构的主要部分上使用基于网络的 IDS。应该由一个系统控制台在网络的一个安全部分中收集所有 IDS 信息。


Web服务器
应用服务器
外部 DNS
服务器
防火墙包括了适当的
规则，以禁止 N-IDS
检测器访问内部网络。
Internet
防火墙
分线器
N-IDS 检测器
安全网络
安全系统控制台

信息安全处理



安全处理项目计划