国瑞数码安全系列丛书

内联网与外联网安全指南

Kaustubh M. Phaltankar 著
杨义先 夏光升 李忠献 译

Implementing Secure Intranets and Extranets

人民邮电出版社
www.pptph.com.cn

内联网与外联网安全指南

[illegible]

国瑞数码安全系列丛书

内联网与外联网安全指南

Kaustubh M.Phaltankar 著

杨义先 夏光升 李忠献 译

人民邮电出版社

图书在版编目（CIP）数据

内联网与外联网安全指南 /（美）费尔坦卡（Phaltankar, K. M.）著；杨义先等译.
—北京：人民邮电出版社，2001.1　　（国端数码安全系列丛书）
ISBN 7-115-09043-2

Ⅰ. 内…　Ⅱ. ①费…　②杨…　Ⅲ. 计算机网络 — 安全技术—指南
Ⅳ. TP393.08-62
中国版本图书馆 CIP 数据核字（2000）第 73224 号

内 容 提 要

本书详细地提供了作者现实的亲身实践经验。重点介绍了有关内联网（又称内特网）和外联网（又称外特网）应用的高灵活性网络和安全基础设施的开发和实施。本书很好地阐述了如何为内联网或外联网构建一个安全、可靠、高性能、高效益的网络和安全基础结构的技术，详细介绍了路由器、交换机、服务器、防火墙等网络关键部分的安全配置。

本书的读者面相当广泛，只要他们对内联网和外联网的实现感兴趣，其中包括：

- 做网络和安全基础结构工作的 IS 和 IT 专业人士；
- 想了解如何选择正确的技术和设备供应商的管理者
- 为因特网、内联网和外联网策略提供技术和商务前景的设计者和创建者；
- 一些想在因特网领域发挥作用的学生和专业人士，他们想了解实现安全内联网和 VPN 通道的内幕。

国瑞数码安全系列丛书

内联网与外联网安全指南

◆ 著　Kaustubh M. Phaltankar
译　杨义先　夏光升　李忠献
责任编辑　陈万寿
◆ 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@pptph.com.cn
网址　http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销
◆ 开本：787×1092　1/16
印张：19.5
字数：486 千字　　2001 年 1 月第 1 版
印数：1－4 000 册　　2001 年 1 月北京第 1 次印刷
著作权合同登记　图字：01－2000－2288 号
ISBN 7-115-09043-2/TN·1688

定价：33.00 元

译 者 的 话

网络信息安全保障迫在眉睫。当前，围绕网络信息安全和信息技术，国家与国家、集团与集团、甚至个人与个人之间展开着日益激烈的冲突。现在世界上每年因利用计算机网络进行犯罪所造成的直接经济损失令人吃惊，利用计算机通过互联网络窃取机密信息的事例也是屡见不鲜。网络信息安全隐患，将全方位地危及社会的经济、政治和文化等各个方面。

当前，我国社会信息化正以一日千里的速度前进，对网络与信息安全的需求日益增大。与其他领域不同，网络与信息安全问题必须依靠我国自己的力量来解决。引进国外产品或照搬国外先进技术来解决信息安全问题无异于引狼入室。为此，国家已经明确规定："信息安全产品一定要立足国内，自主开发"。

当前国内在网络与信息安全方面的基础（人员和技术）还相当薄弱，急需加强。"在游泳中学游泳"，将国际上最新出版的一些著作翻译后介绍给广大读者，是使国内同行更好更快地了解国际上在信息网络安全方面的最新进展的最佳途径之一。为了取得更好的效果，人民邮电出版社与北京邮电大学信息安全中心和天津市国瑞数码安全系统有限公司共同合作翻译出版了这套"国瑞数码安全系列丛书"。希望本系列丛书能够为促进我国的网络信息安全做出一定的贡献。

天津市国瑞数码安全系统有限公司（http://www.ncs-cyber.com）是一家以网络安全和信息安全为主的民族高科技企业，公司致力于为我国社会信息化提供全方位的网络安全和信息安全保障。公司拥有一大批国内一流的密码学和信息网络安全专家，硕士、博士学位获得者超过公司员工总数的一半，公司真诚地欢迎更多的有志于我国数码安全的专家加盟（联系电话：010-62383780、022-27237081）。公司已经开发出具有完全自主知识产权的众多信息与网络安全产品。比如：B2B 电子商务安全平台、电子商务加速卡、网站卫士、安全替音电话、WAP 安全解决方案、宽频系统安全结构和多种加密卡及加密算法等。

北京邮电大学信息安全中心(http:\\www.bupt.edu.cn)是国务院学位委员会正式批准的全国仅有的三个"密码学"博士点之一，长期致力于网络信息安全的理论和关键技术研究。欢迎有志青年来此攻读硕士、博士和博士后。

本丛书还得到了国家高等学校骨干教授资助计划项目（国家教育部）、国家重点基础研究发展规划项目(编号: G1999035805)、国家杰出青年基金项目（批准号：69425001）、国家自然科学基金项目(批准号:69882002，60073049)的资助。特此致谢。

序

在美国和任何其他地方，计算机通信作为商业贸易中举足轻重的组成部分，已经成为商业的必需。因特网伴随着诸如电子邮件和 WWW 服务等主要应用成为这个热潮中的重要部分。电子商务正在以专有 Web 页的数字关系把公司、顾客和供应商联系起来。这并不奇怪，因此，安全问题对于每一个依靠计算机通信进行日常商务的人来说已经变得越来越重要。

“安全”是一个经常被提到的名词，对很多人意味着很多东西。对于某些人来说，它代表秘密通信，对于某些人来说则是交换的完整性和真实性，而对于其他人来说意味着不受干扰、侵犯和不会被拒绝服务。事实上，安全是所有这些和更多的东西。安全技术与网络信息体系结构具有很密切的关系，从专用电路的保护到合作方之间交换信息的保护，都涉及到安全技术。

本书中，Kaustubh Phaltankar 探索了很多细节和特性，给出了在多方共享的网络底层上设计、构建和提供安全的虚拟专用网络（VPN）的具体方法。这些共享的多方包括公司内联网（应用因特网技术的 VPN）和外联网（很像内联网，只不过各参与者是分离的实体）。

值得说明的一点是，安全网络工程还是一个正在进步中的工程。从技术上讲，它有可能提供端到端密码安全，以防止第三方截收和修改两终端实体之间的通信。然而，为了达到这个目的，需要固定的加密算法、特定的密码密钥分配体系和其他有关安全方面的特性。关于这些功能的规则还没在各有关实体中完全达成一致。然而，在企业网中，安全技术的投资一向很可观，现在似乎该收获了。

把这些想法实施于多层网络环境中要求与因特网工程任务组（IETF）以及各种安全服务中的商务公钥结构相类似的概念。

对安全方面能力的需求正在快速增长，这一点不容置疑，尤其是 IPv6 的出现将人们的注意力集中到 IPSEC，即 IETF 的获取端到端信息包模式安全性的思路上来。

本书除了为读者提供必要的技术之外，实例分析属于本书对时下网络安全领域所做贡献中最有价值的一部分。了解真实世界中实际的公司如何解决现实的安全挑战，这将是读者从这本书中能够得到的最有用的经验之一。

Vinton G.Cerf

Camelot 1999

（Cerf 博士为 MCI WorldCom 公司高级副总裁，被称为“因特网之父”。——编者注）

前　言

百闻不如一见
百见不如一试
孔子

我个人一生都会追随上面这句名言。因此，它对我从理论走到实践中去是很重要的。我想这是我成为工程师的一个原因。在我的职业生涯和这本书中我将继续遵守这句名言。我把这本书写成引导型，而非入门型。本书三分之一以上是实例研究，理论部分有丰富的实际思想和基于我个人经验的技巧。

在 1995 年，因特网成为时代主流之前，我就一直从事因特网方面工作。从那时起，遨游于因特网就成了永无休止的乐趣和工作。这种乐趣现在成为很多机构的重要使命。在过去的两年里，问题已经从“因特网为商务做好准备了吗？”转移到“商务为因特网做好准备了吗？”。当各团体认识到因特网的力量和类似因特网协议（IP）和 Web 页的因特网技术时，大量的商业应用在一夜之间铺天盖地蜂拥而至。在领导这场高速信息流、高生产率、高利润的冲锋中，内联网和外联网的应用占据着中心舞台。出版社、杂志和贸易期刊的好多文章都肯定了一点，那就是商务已为因特网做好了准备，而且在这个新的前沿阵地中走在了前面，抓住了挑战时机。随着商家对商家（B to B）电子商务的初步成功，商家已采用外联网技术，并以因特网作为无所不在的传媒。

在过去的两年中，很多阐述如何建立一个因特网或内联网商务应用的书籍出现了。这些书作了一项非常好的工作，即向读者介绍了创建这些系统的管理和应用方面的知识。一旦管理在概念上完成了，在开发和实施这些应用时还有很多非常重要的工作要做。在这些应用被实施于内联网和外联网环境之前，必要的网络和安全基础设施必须到位。本书正好满足这个需要。

本书的焦点是提供现实的亲身实践资料，这些资料是有关内联网（又称内特网）和外联网（又称外特网）应用的高灵活性网络和安全基础设施的开发和实施的。本书回答了下列几个问题：

- 如何为内联网或外联网构建一个安全、可靠、高性能、高效益的网络和安全基础结构？
- 如何配置各种网络和安全的元素，例如路由器、交换机、服务器、防火墙，以达到上述目的。

本书包含了丰富的基于实践经验的建议。它遵循一个逻辑过程，提供开发一个可扩展且可靠的网络和安全基础结构的所有模块。实例分析突出了这个原则，它通过一步步构建公司的内联网使一个假想的公司从一个地区性公司发展成一个全球性公司我们的重点放在以下几个方面：现存网络和应用集成，以及为工作地点不固定的雇员、远程机、外联网合作伙伴提供远程访问的 VPN 技术。实例分析集中体现了“百见不如一试”这个原则，它提供路由器、防火墙、服务器和 VPN 设备的完整配置。每个实例分析都建立在前一个实例分析的基础之上。每个实例都把最流行的技术应用于局域网（LAN）、广域网（WAN）、路由器、防火墙和 VPN。所有这些实例都采用了诸如 Cisco、Checkpoint、Motorola 和 Aventail 等领先

供货商提供的产品。

读者对象

本书的读者面相当广泛，只要他们对内联网和外联网的实现感兴趣，其中包括：

- 做网络和安全基础结构工作的 IS 和 IT 专业人士；
- 想了解如何选择正确的技术和供货商的管理者；
- 为因特网、内联网和外联网策略提供技术和商务前景的设计者和创建者；
- 一些想在因特网领域发挥作用的学生和专业人士，他们想了解实现安全内联网和 VPN 通道的内幕。

怎样阅读本书

本书首先提供技术方面的内容，后随一些实例分析。每一章可单独或连续阅读。

- 第一章，概述：介绍了因特网、内联网和外联网的概念。本章探讨了内联网站点连接的传统方法和基于帧中继和因特网 VPN 的新方法。在本章结束时我们介绍了外联网以及它的优势和安全需求。
- 第二章，广域网组件：讨论构建地区或全球外联网和内联网的有灵活性的 WAN 连接的设计选择。本章尽述了 WAN 技术和拓扑结构。
- 第三章，局域网组件：讨论构建有灵活性的 LAN 结构的设计选择。伴随着 LAN 路由协议，出现了各式各样的 LAN 技术，例如，以太网、快速以太网、千兆比特（Gbit）以太网、异步传输模式（ATM）、光纤分布式数据接口（FDDI）、令牌环和 LAN 交换等。其目的是为了提供各种 LAN 设计和选择标准。
- 第四章，网络与服务管理：描述内联网或外联网服务中的网络与服务管理所需要的技术，包括对简单网络管理协议（SNMP）和监控内部和外部服务等级协商（SLA）的远程监察管理资料基本原则（RMON MIBS）的讨论。
- 第五章，内联网和外联网的安全组件：介绍安全内联网和外联网结构和配置的重要元素。我们从安全框架开始讨论，然后探讨可提供数据安全、访问控制和认证的技术。接下来介绍了数字证书的概念，以及对公钥基础结构（PKI）的应用、全局目录、全球唯一签名解决方法的讨论，及对不同类型防火墙和网络地址变换（NAT）的应用的讨论。
- 第六章，虚拟专用网络（VPN）：本章对什么是 VPN、为什么构建 VPN、怎样构建 VPN 作了广泛的讨论。此讨论伴随着一个具体项目面展开。项目中的 VPN 技术都是当前市场上可获得的技术，它们在开放系统互连（OSI）模型的多个层面上都是可行的。这些技术包括 IP 安全协议（IPSec）、GRE 隧道、点到点的隧道协议（PPTP）、局域网对局域网的 L2TP 隧道协议，以及在公共因特网上的拨号 VPN 连接。
- 第七章，实例分析：实例分析为读者提供内联网和外联网网络和安全基础结构在实际中的实现。实例分析还为读者提供了设备安装和配置方面的详细知识，具体有以下设备：路由器、交换机、远程控制设备、带有 IPSec 的因特网 VPN、VPN 客户机、VPN 服务器、永久性虚拟电路（PVC）的帧延迟和传统环境中的 SNA 网关。

本书中还有大量的实用资料可以直接应用到你的环境中去。虽然我企图涵盖所有最典

型的方案，但你的情况也许更特殊。本书中的概念、理论、实例、参考资料将会提供足够多的资料来制定满足你个人需求的解决方案。

网址

网址：http：//www.netplexus.com/artechhouse 将提供进一步的数据。此网站能让我们维持一个有关本书中所有讨论过的论题信息的动态知识宝库。因特网和因特网技术每天都在发展，并为企业的内联网和外联网的成长提供了动力。此网站还可以让你了解到最新的有关技术和产品的信息，这会对你的内联网和外联网的实现有所帮助。我希望你会发现这个站点很有用，欢迎提出批评意见和反馈信息。

致谢

我必须感谢我的所有的团队，包括 MCI 和后来的 Cable&Wireless，他们提供了连续不断的学习环境，鼓励每个人到实践中去。我还要特别感谢我的良师益友 Dick Stephens 和 Randy Catoe，我在 MCI 的日子里他们一直支持我。Jim Martin 和主机中心业务团队一直提供用户反馈意见，使技术工作为用户服务。来自安全工程的 Dale Drew 和 Steve Weeber 在我进入安全领域时给了我最早的支持和帮助，而 Dr.Abdou Youssef 在实例分析方面提供了详细的反馈资料。特别感谢 MCI 的 Dr.Vint Cerf 和 John Clenson，每一次和他们的交谈都让我认识到我还有许多知识要学。

我还想感谢 Artech House 的组稿编辑 Mark Walsh 和 Barbara Lovenvirth，在漫长的底稿编写过程中他们一直对我保持耐心。最后，最重要的是，我要感谢我的妻子 Shadong，因为她一直鼓励我完成这个计划，尽管我们都在期待着我们的第一个孩子的出生。没有她的帮助和鼓舞，这项计划也许永远只是我的一个梦想而已！

约定

a．用到的图形符号

主机

工作站

服务器

用户工作站

接线器

LAN/WAN 网络

b. 类型约定

no ip　　表示路由器命令

The interface　　表示说明、备注

Kaustubh Phaltankar
E-mail：kaus@netplexus.com
网址：www.netplexus.com

目　录

第一章 概 述

本章我们将定义几个术语：因特网、内联网与外联网，并针对每种情况各举几个例子。首先，我们简要说一下“因特网”与“因特网技术”的区别，然后详细分析与内联网和外联网有关的技术和概念，再集中精力讨论内联网和外联网的优势，最后是它们各自的网络需求和安全需求，以及各种可选的应用方式。

定义：

因特网：是由分布在全球的无数个互联的网络组成的全球网。它把私有网络、公共网络以及校园网连接成一个整体。

内联网（又称为内特网）：是私有的企业网。它利用因特网技术和 Web 技术为企业内部提供信息收集和分发服务。

外联网（又称为外特网）：是由利益联系而组成的群体所共有的企业网，它由内联网扩展而来，把内联网扩展到企业外所选定的多个实体。

1.1 因特网

本书中，我们假设读者已经比较熟悉因特网并阅读过很多有关其起源与发展的文献书籍。这样我们对因特网就只略做介绍，然后把精力集中在内联网和外联网上。

如上面所定义的，因特网是由互相连接的网络组成的全球网，如图 1.1 所示。

因特网是由无数个私有网络、公有网络及校园网组成的。这些网络通过各种私有或公共的接入点互连，这些接入点又称为等同点。其中公共等同点又称为网络接入点，即 NAP。因特网服务提供者（ISP）根据其网络规模及容量可分为 3 个等级。一类 ISP 如 UUNet、GTE、Sprint 以及 Cable&Wireless 等，他们拥有巨大的因特网骨干网，容量为多个 OC-12（655Mbit/s）或 OC-48（2.4Gbit/s）。大多数一类 ISP 都与 NAP 有连接，以使较小的 ISP 能从 NAP 接入大 ISP 的网络。NAP 是与因特网上其他网络通信的最省钱的方式。由于应用广泛，因特网上的 NAP 已经有些拥挤了。解决这一问题的方法之一就是在选定的服务提供者间建立私有的等同安排。例如，如果某个一类 ISP 与某个二类 ISP 间的通信满足该一类 ISP 的可接受使用政策（AUP），则这两个 ISP 间就可以建设一个私有等同。它可以建设在 NAP 或该一类 ISP 的存在点（POP）处。

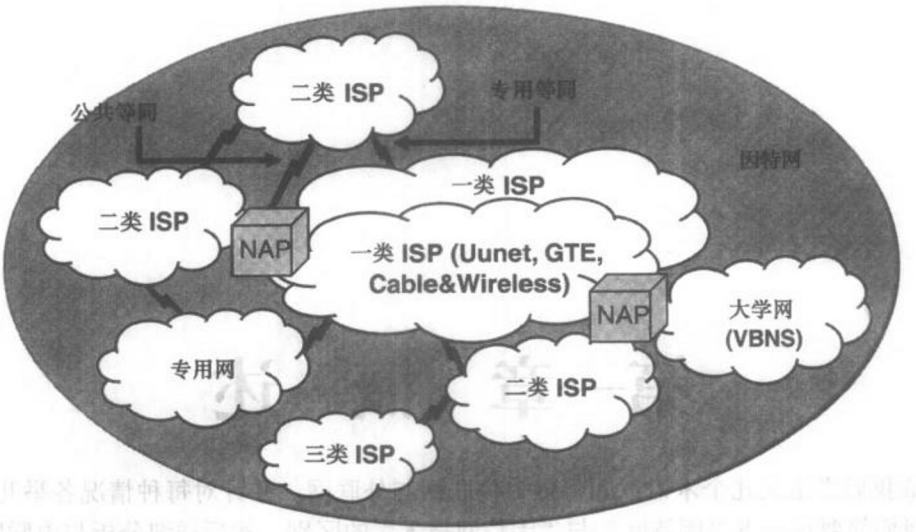

图 1.1 全球因特网的网络结构

注释：对企业来说，同时保持对 ISP（一个或多个）的多条连接是个好主意。最好的办法是用专线连接多个 ISP，并通过负载平衡充分利用各条专线。如果你的通信负载不大，用不了两条专线时，可以选择 ISDN 或 PSTN 拨号上网方式作为后备，当专线容量达到某一限度或断线时自动激活，使通信负载转移到后备方式上。

在讨论内联网的定义之前，先来说明“因特网”与“因特网技术”间的重要区别：“因特网”指的是前面所说的全球网络；而“因特网技术”则是一系列因特网协议与应用的总称。TCP/IP 协议是因特网网络传输的基础，另外因特网上还有一些基于 TCP/IP 的应用协议，如 SMTP（简单邮件传输协议）、POP3（邮局协议）、Telnet（用于远程登录）、FTP（文件传输协议，用于交换数据文件）。这些协议与应用就总称为因特网技术。

另外一个常常与因特网技术一起使用的术语是“Web 技术”。“Web 技术”指利用 HTTP 传输、用 HTML/XML 表示 Web 数据的技术。HTTP 协议建立在 TCP/IP 协议之上。Web 服务器与 Web 客户（比如，Netscape 浏览器）通过 HTTP 协议通信。Web 服务器的信息在 Web 客户端以 HTML/XML 标记的形式出现。由于 Web 接口的广泛普及和浏览器的低廉价格，Web 浏览器已经成为广为接受的客户端桌面接口。

下面，我们将深入讨论内联网的定义以及建立内联网解决方案的典型技术。

1.2 内联网

企业内联网的巨大作用已经为其早期使用者和技术先驱们所证实，而内联网前进的步伐也在加快。如 Geoffrey Moore 所说，在使用内联网的历程中，我们正在跨越鸿沟，将这一“早期市场”从“主流市场”中分离出来。2000 到 2001 年主流市场的增长将为这一市场带来极大的增长。

最早期的内联网主要用于：

- 在部门内部公布信息，以使员工更容易访问内部数据；

- 建立员工自助服务 Web 站点，提供人力资源、工资单、市场销售以及培训等服务。

随着对这一技术的进一步了解，企业又把内联网用于一些更为复杂的服务，如：

- 分工协作管理、制定计划、发布消息以及建立讨论组；
- 库存及后勤管理系统；
- 用户服务管理系统。

一个成功建设的内联网可以使企业：

- 省钱；
- 提高员工生产效率及员工稳定度；
- 提供更好的用户服务，增加顾客满意度并留住顾客；
- 使产品信息、生产计划和产品竞争力分析等工作更加方便快捷。从而获得竞争优势，以及更多的销售额、更多的年产值、更多顾客。

在大多数企业中，内联网最初只用于少数部门，随即迅速扩展到整个企业，而使得企业里各部门间的种种不同信息泛滥成灾。企业认识到这种不加控制的扩展对企业弊大于利，于是开始制定整个企业的分散化信息管理的策略。从而形成统一的信息发布机制，同时也保留了一些原来的扩展策略，以使企业能充分利用内联网的力量。

企业内联网可能基于因特网技术、Web 技术或产品供应商私有的技术。有些企业的内部网完全基于私有网络协议。比如 IBM 的源路由桥接（SRB）、Novell 的 IPX 协议。虽然这些网络具有完备的功能，但其私有性使得协议费用昂贵、用户界面不直观、而且扩展能力有限，因而不能充分利用企业的全部资源。这些不利因素现在都可以用标准协议来解决，如，TCP/IP、HTTP、HTML 等。私有协议的支持者，尤其是产品供应商在这方面已经有过深刻教训。IBM 和曾经是网络巨人的 Novell 的市场占有率已经落在了 Sun 和 Mircosoft 之后，而后两者都支持开放式标准。现在，那些曾经靠其私有协议和技术获利的企业也开始采用标准的因特网协议。这正应了一句俗话："如果你不能打倒他们，就加入他们"。这些厂商希望由此阻止市场占有额的下滑，并利用因特网和因特网技术的流行性。例如，Novell 公司已经在 Novell 5.0 中引入了全 IP 支持，IBM 也开始在其主机中支持 TCP/IP。有些供应商，如 Open Connect，也在 IBM SNA 网关中引入 IP，以使用户能通过 Web 访问过去隐藏在私有技术后面的数据。

建立成功的内联网的先决条件是什么呢？

- 统一的内联网策略和结构；
- 企业间安全、多方位的连接；
- 与原有的网络和应用（包括主机）相结合；
- 使用基于标准的网络技术、安全技术和 Web 认证技术；
- 基于通用的 Web 客户端的通用用户界面，以减少维护每个终端的费用；
- 在网络访问、安全、内容审查及管理等各方面使用统一的企业政策与方针；
- 管理和用户大宗买进。

考虑到上述设计要求，我们来探究建立安全内联网的各种方法。首先我们来考虑传统的专线方式，然后是帧中继方式，最后讨论用基于因特网的 VPN 方式来建设安全内联网。

1.2.1 传统方式

建立一个成功的内联网的重要要求之一是"企业内部之间安全、多方位的连接"。也就是