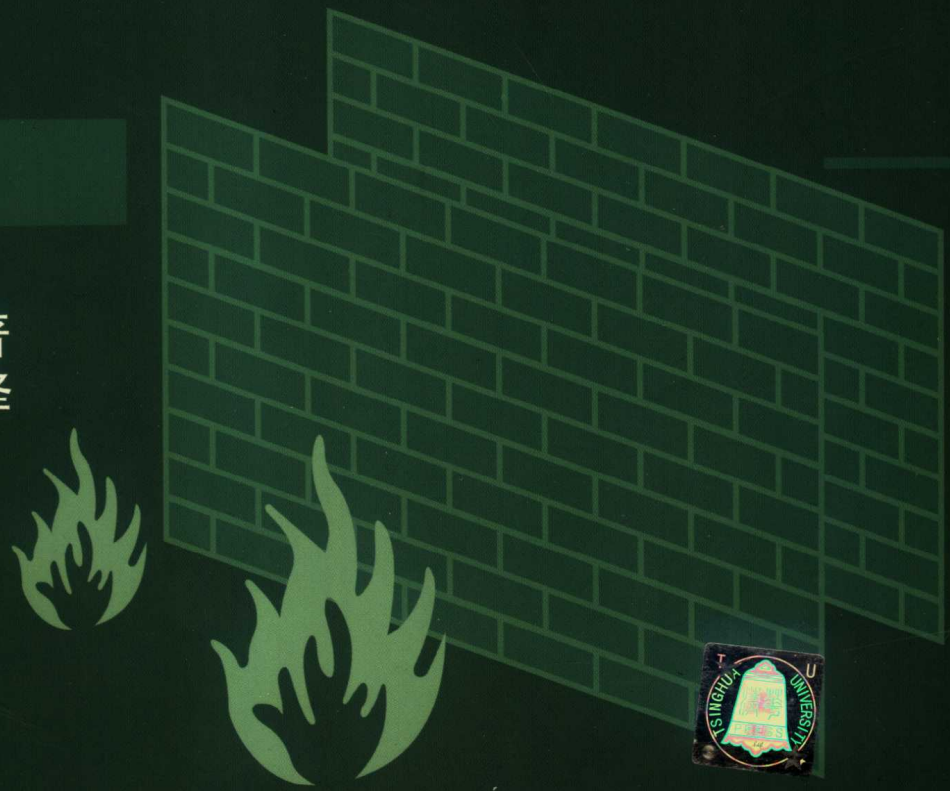
THOMSON

Internet Security and Firewalls

Internet安全与防火墙



V.V.Preetham 著
冉晓旻 等译

清华大学出版社

Internet 安全与防火墙

V.V.Preetham 著

冉晓旻 等译

清华大学出版社

北 京

V.V.Preetham
Internet Security and Firewalls
EISBN: 1-931841-97-7

图书在版编目(CIP)数据

Internet 安全与防火墙/(美)普端萨姆(Preetham, V. V.)著；冉晓旻等译. —北京：清华大学出版社，2004.6
书名原文：Internet Security and Firewalls
ISBN 7-302-08523-4

Ⅰ. I…　Ⅱ. ①普…　②冉…　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（2004）第 037059 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大夏
http://www.tup.com.cn　　**邮　　编**：100084
社总机：010-62770175　　**客户服务**：010-62776969
责任编辑：冯志强
封面设计：付剑飞
印 装 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：14.25　**字数**：351 千字
版　　次：2004 年 6 月第 1 版　2004 年 6 月第 1 次印刷
书　　号：ISBN 7-302-08523-4/TP・6124
印　　数：1~4 000
定　　价：26.00 元

致　　谢

非常感谢 Vineet Whig 和他在 NIIT Ltd 的开发小组在本书编写过程中提供的出色的支持、协调和指导。在编写本书过程中我与 NIIT 的 Anita Sastry、Kuljit Kaur 和 Nitin Pandey 的合作非常愉快。

在此我要专门感谢 Stacy Hiquet，他策划了本书。还要感谢项目编辑 Cathleen Snyder，没有其大力帮助，本书就难以达到现有的水平！最后，还要感谢 Priyanka 绘制了本书的插图。

NIIT 简介

NIIT 是在全球 38 个国家开展业务的 Global IT Solutions Corporation。NIIT 具有独特的业务模式和技术创新能力，它可以向全球 1000 多家客户发行软件和学习解决方案。

NIIT 培训解决方案的成功在于其独特的教育方法。NIIT 的 Knowledge Solutions Business 策划、研究和开发了各种教学材料。他们按照富有活力的教学设计方法，编写了吸引人、并富于挑战性的课程内容。NIIT 具有全球最大的学习材料开发设施，他们已经积累下了多年对 5000 余人进行培训的经验。

NIIT 在信息技术领域每年培训超过 200000 人，他们使用了持久的教学方法、视频辅助教学方法、基于计算机的培训（CBT）和基于 Internet 的培训（IBT）。NIIT 创造了一年内培训人数的世界吉尼斯记录！

NIIT 已经开发了超过 10000 学时的教师授课式教学（ILT），超过 3000 学时的基于 Internet 和计算机的培训。IDC 将 NIIT 评为 2000 年度全球顶尖的 15 家 IT 培训提供商之一。NIIT 的教学方法富有独创性，他们的教学团队热衷于教学研究和开发，他们是过去 20 年计算机教育和培训领域的先锋。

NIIT 视质量为第一。其大多数培训程序都通过了 ISO-9001 认证。NIIT 是被评估为全球 SEI-CMM 的 Level 5 的第 12 名公司。NIIT 的 Content（Learing Material）Development 设施是全球第一个达到最高成熟度认证的教学设施。NIIT 还与 Computer Associates、IBM、Microsoft、Oracle 和 Sun Microsystems 等公司建立了战略伙伴关系。

作者介绍

V.V.Preetham 是位于 Georgia 的 Atlanta 的 ConceptUniv 的 Chief Architect。他还是 Sun Certified Architect、Sun Certitied Java Programmer、BEA WebLogic Enterprise Developer、CIW Enterprise Developer 和 Microsoft Certified Product Specialist。他还是 IBM 关于 WebSphere 3.5、Visual Age、XML 和 UML 方面的认证专家。他编写过 *Java Web Services Programming*。目前他从事的工作涉及咨询、研究和开发。V.V.精通 C、C++、C#和 Java。他对于 Internet 协议、联网协议和 J2EE 的 OMG 也有广泛的研究。

前　言

随着企业日常工作中广泛使用 Internet，各种企业越来越需要保护自己的网络安全。如果出现了网络安全问题，将会给公司造成严重的经济损失和客户损失。

我们可以使用防火墙来有效地保护企业网络的安全，防火墙提供了外部网络和内部网络之间的保护层。本书深入介绍了防火墙及其实现的知识。

- 第 1 章简要介绍了 Internet、OSI 模型和 TCP/IP。
- 第 2 章讲解了基本的安全概念，比如加密学和数字证书，以及常见的安全隐患，比如网络扫描和网络攻击。
- 第 3 章介绍防火墙及其类型、用法和局限性。
- 第 4 章接着第 3 章的内容继续讨论，介绍防火墙技术，比如代理服务器和虚拟专用网络。
- 第 5 章介绍防火墙体系结构，包括了各种根据具体网络要求采用的体系结构。
- 第 6 章讨论创建安全策略的步骤，市面上的防火墙产品和评估防火墙的标准。
- 第 7 章内容以第 6 章内容为基础，继续讨论安全和配置防护主机的步骤。
- 第 8 章研究了防火墙在保护 Internet 上各种服务（包括 Web、FTP 和电子邮件）安全的作用。
- 第 9 章解释了网络入侵的法律后果。

本书译者是计算机和网络安全方面的专业人员，具有深厚的专业背景和良好的英语素养，本书必将成为希望学习防火墙知识的读者的良师益友。参与本书翻译工作的人员还有唐有明、王俊伟、吴军希、李振、郭军威、李有军、朱俊成、张瑞萍、吴东伟、李洪海、李乃文、靳军等。由于译者水平有限，书中不妥之处在所难免，欢迎广大读者批评指正。

目　录

第 1 章　Internet 概述

Internet 是历史上最重要的发明之一。多年以来，它已经使人们的交流和商业交易方式发生了巨大变化。本章解释了 Internet 的基本概念以及它的工作原理，概述了 Internet 的历史和发展年表，并解释了 Internet 的主干协议 TCP/IP（传输控制协议/网际协议）。此外，本章还说明了 Internet 的当前趋势，以及它对未来发展的影响。

1.1　Internet 的基本概念

Internet 是允许通信达到一个新的高度的主要影响因素。通信是任何事务处理的实质。在早期，人们常常将消息系在鸽子腿上，希望它们能够飞到收信人那里。这并不容易，因为人们必须将鸽子训练为信使来完成这个任务。就通信方式的演化来说，已经创造了两个重大的技术突破——电报和电话。那时，电报和电话是最实用的端到端通信技术。

另外还存在对取代报纸的另一种有效方案的潜在需求。报纸是一种广播媒介，而不是像电话那样的端到端的实时通信媒介。收音机和电视机的出现彻底改变了广播和出版行业。

当广播和电信媒介为人类提供了信息和娱乐时，Internet 慢慢开始成为替代它们的通信手段。随着对联网技术的研究越来越多，人们意识到这类网络在邮件、端到端通信和广播代理方面的潜能。Internet 现在已经成为各类通信（无论是一对一、一对多，还是多对多）的主要媒介。

就定义而言，Internet 是用互连计算系统横跨世界的巨大网络。这些系统是“可以定义为拥有计算的基本质量的实体”的设备。它们的范围可以从照相机到巨型计算机。几乎可以准确地说 Internet 还跨越了外太空，因为它是由人造卫星（可以浏览和监控不同的行星）等设备构成的。

Internet 扩展到如此巨大的网络要归功于政府、工商界和学术界的共同努力。如果没有这三方面因素的影响，Internet 可能不会发展到跨越地理和政治界线的规模。世界上任何一个角落中的任何人都可以在 Internet 上分享他或者她的观点。地球两端的人可以交流彼此的思想。反过来，这又加快了改革进程。以 Internet 速度传播信息是新技术突破的另一个原因。

1.1.1　Internet 的历史

Internet 是数百万个出于某种目的、相互连接在一起的不同计算设备的生机勃勃的系统。最初，为了在几台计算机之间交换军事信息设计了 Internet。慢慢地，大学发现 Internet 是共享学院实验室中进行的研究的有关信息的更快捷方式，并且它从几台计算机发展为几百台计算机。之后，工商界对网络上共享的信息感到好奇。Internet 变得在一个方面或者另

一个方面更适用于每一个团体。毫无疑问，Internet 发展的主题是“信息共享”。几乎每个人都受益于这种网络的发展。以电子介质的速度传播信息已经成为几乎每个人的基本需求。Internet 跨越政治和地理界线的发展和普遍接受是“电子共享数据和信息已经成为必需品，而不仅仅是应用”的标志。

本书后续小节介绍了 Internet 历史中发生的事件的年表，从而帮助你了解它的起源和发展。年表概述了几十年来发生的、并且影响了 Internet 发展的事件。

1. 20 世纪 50 年代

引发 Internet 概念的主要事件之一是前苏联发射的第一颗人造地球卫星。该卫星称为 Sputnik，并且该事件导致美国国防部内成立了 ARPA（高级研究计划局）。

2. 20 世纪 60 年代

许多与网络有关的研究都是在 20 世纪 60 年代进行的。ARPA 开始研究分时计算机之间的网络互联。许多大学开始进行联网方面的研究。在这个时期，许多论文提出了关于联网的不同理论。此外，电信巨头们也开始研究和开发现有电信线路上的计算机网络。起草了第一个 ARPA 网络计划（称为 ARPANET，高级研究计划局网络）。ARPANET 是世界上第一个主要的分组交换网络。

3. 20 世纪 70 年代

在 20 世纪 70 年代，ARPANET 扩展为包括研究实验室和大学中存在的许多不同网络。第一个电子邮件计划是在 20 世纪 70 年代早期构思的，同时还有文本聊天应用程序。创建了 Telnet 和 FTP（文件传输协议）的 RFC（请求注解）。以太网作为联网协议的概念形成，并且出现了以 TCP 和 IP 作为传输和通信协议的概念。

注意：以太网是使用最广泛的 LAN 技术。通常，以太网使用同轴电缆；无线 LAN 中也使用以太网。TCP 和 IP（连在一起作为 TCP/IP 使用）是 Internet 的协议。专用网络中也使用它们。

4. 20 世纪 80 年代

许多网络是在 20 世纪 80 年代形成的，包括 BITNET、MILNET、CSNET、NSFNET、UUNET 和 USENET。TCP/IP 是在其中许多网络上通信的主干协议。这一时期提交了许多 RFC，影响了在不同子网之间互连的发展。此外，在线形成了许多新闻组。

术语“Internet”成为暗示网络是由许多子网组成的事实表现。大学站点和商业配置了许多基于 UNIX 的台式计算机。DNS（域名服务器）被引入来管理 Internet 主机在网络和子网之间的命名。在 20 世纪 80 年代早期，由于计算机设计的缺陷，偶然将病毒引入到了网络中。这类事件最初使整个 Internet 停滞不前。但是，Internet 在 80 年代后半期稳定性较好，同期还爆发了 Internet 蠕虫病毒。在 80 年代末，多个国家有大约 100 000 台主机连接到 Internet。

5. 20 世纪 90 年代

ARPANET 是在 20 世纪 90 年代退出历史舞台的。跨越多个国家的不同子网之间的连接在不断增加。CERN（欧洲原子核研究组织）引入了 WWW（World Wide Web）。一些国家形成了与 Internet 相关的法律。一些国家研究了保密技术以保护 Internet。连接的基础结构以加速度发展。许多网络被引入到更宽的带宽连接上，从 1.5Mbps 的 T1 线路到 45Mbps

的 T3 线路。总的来说，Internet 的容量（带宽）也在这一时期得到了改善。

发生了 Internet 应用中的许多重大改变。电子邮件广泛应用于更快的通信。人们可以买得起 PC。许多台式系统和 PC 连接到 Internet。创建了 InterNIC（Internet 网络信息中心）来监控 Web 网上的目录、注册和信息服务。许多团体（包括大学、学院、图书馆、新闻组、公告牌和一些国家的政府）开始树立他们在 Web 网上的形象。

许多 ISP 在网络上建立他们的商业，提供到不同社区的拨号接入。由于 ISP（因特网服务提供商），PC 和电话线的使用呈指数增长。形成了浏览 Web 网的概念。引入了许多脚本语言来表示 Internet 上的信息，并且 HTML 成为表示 Web 网上信息的事实标准。

这一时期提出了数千个 RFC。许多组织开始在网络上进行商业活动。20 世纪 90 年代后期引入了电子商务。股票交易、金融、银行业务、制造业、供给链以及其他许多不同的行业团体开始参与在线商务。

分布式计算（计算资源的共享）也成为科研人员利用 Internet 聚合能力的焦点。通过暴露网络和网络相关资源中的安全漏洞，黑客变得越来越引人注目。Internet 安全几乎成为每个使用网络的人的主要忧虑。发明了许多技术和协议来保护 Internet。小到手表或者手机的设备也开始分享 Internet 空间。发明了移动 Internet 计算。由于 Y2K 故障，20 世纪 90 年代后期还成为使用计算机的每个商业的紧迫时期。许多 Internet 资源被升级以克服 Y2K 问题。Internet 的使用呈指数增长（主机的数量级为数百万台）。Internet 最终发展为更加稳定和更加可靠。

6．现在

几乎已经用完了 TCP/IP 地址系统。新的协议（例如 IPv6，有更多的地址空间）可以解决这一问题。网络商务正在呈指数速率增长。人们对在 Internet 上进行商务和交易的信任正在按小时增加。连接到 Internet 的主机数正在惊人地增加。正在以加速度消耗基础结构的容量。

商业和人类对于 Internet 的依赖几乎是令人吃惊的。如果 Internet 在某一时刻中断了，那么许多商业和一些将它们的大部分服务依赖于 Internet 的发达国家就会终结。黑客、病毒、蠕虫和私人入侵是使用 Internet 的每个人的主要焦虑。现在投入的大部分资金用于研究较好的 Internet 安全技术。

在 Web 网上使用各种各样的介质内容（例如视频流、电话和高清晰度电视 HDTV）。普通用户（有 PC 和电话线）要求以更宽的带宽来访问 Internet 上的介质内容。拨号带宽正在增加。普通用户渐渐可以使用速度高达 600Kbps 的 ISDN 和 DSL 连接。

总的来说，网络不仅仅是通信骨干，而且还是文件服务器、计算机服务器和应用服务器。换句话说，文件、计算资源和分布式应用在网络上的共享正在呈指数增长。新的互连范例和分布式联网技术正在发展。网络扩展是如此的令人难以置信：考虑一个没有这类完全包含概念的世界几乎是不可能的。

1.1.2　基本的 Internet 介绍

术语“Internet”源于两个词根——“inter（在中间）”和“network（网络）”。互连两个网络的能力引入了 Internet 的定义。Internet 与网络有什么区别呢？其实没有太大区别。

网络是由许多计算设备组成的，如图 1.1 所示。

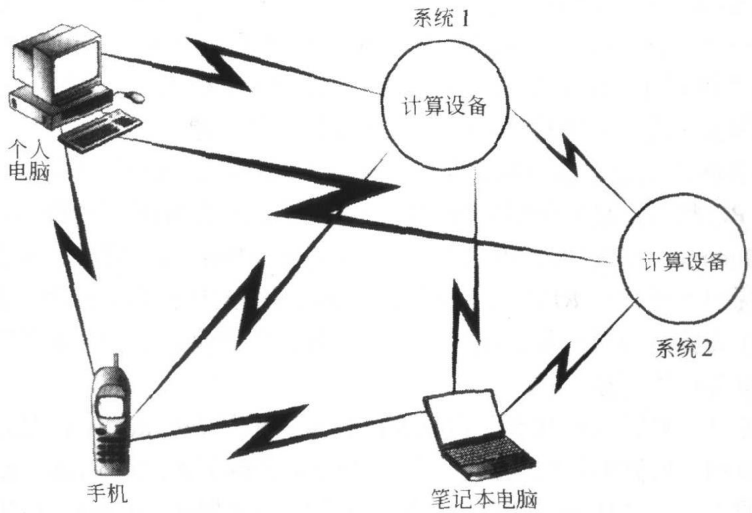


图 1.1 拥有不同计算设备的网络

网络还可以是由许多子网组成的，如图 1.2 所示。

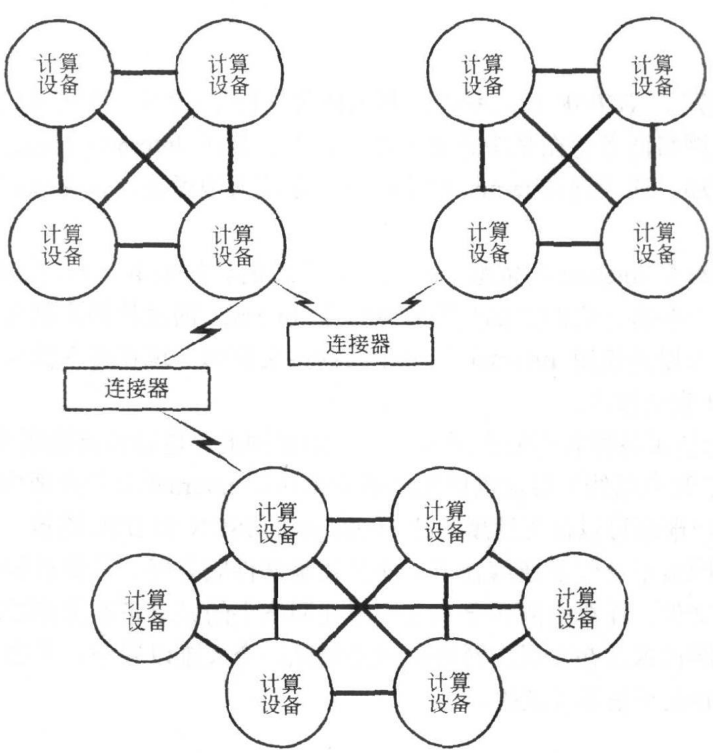


图 1.2 具有子网的网络

Internet 是所有网络之母。当将这类大网络和子网相互连接时，你就会有效地得到 Internet，如图 1.3 所示。

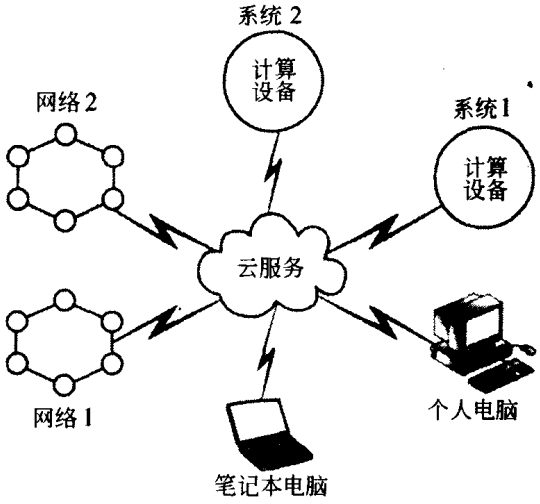


图 1.3　网络和子网构成了 Internet

Internet 的初期只有一个目的——开发不同计算设备之间的战略性军事通信。基本需求是在军事基地之间共享信息，从而准确和有效地部署军事战略。

当 DARPA（国防部高级研究计划局，美国军事研究机构）试验 ARPANET 时，提议是要拿出一个在战争期间既耐用又可靠的简单网络。尽管还有其他许多目的，但是这是最重要的原则。在设计网络时，目的之一是确保没有集中式命令和控制单元，这样就不会存在敌人导弹有可能破坏整个网络的单个攻击点。但是，创建一个没有集中式权威机构的有效联网系统几乎是不可能的。

ARPANET 在选择分组交换通信作为它的主要协议之前，还尝试了不同的设计。最终选择分组交换的原因很简单。分组交换网络赋予了他们想要的耐用性和可靠性。首先，网络是由多个节点组成的。每个节点有一个节点地址，并且有足够的智能来管理自己的状态和有效地将它的状态和可用性通知给其他的对等节点。每个节点都是直接或者间接地连接到网络中的其他各个节点。因此，源节点可以通过多条路径到达任何一个特定的目的节点。

不论源节点何时想与目的节点通信，它都可以用数据包形式将信息发送给目的节点。数据包是由信息组成的小包，包括源地址、目的地址和必须从源发送到目的地的信息。数据包的大小通常不变。换句话说，如果特定协议的数据包大小固定为 1 个字节，那么发送 100 个字节的信息需要 100 个 1 字节数据包。这就是如何将大量信息分割成许多数据包、从而将它从一个节点发送到另一个节点的示例。

在这个示例中，如果要从源节点向目的节点发送 100 个字节的信息，那么每个数据包都包含相同的源地址和目的地址，分别代表产生这些数据包的节点和它们将要到达的节点。然后，源节点将这些数据包发送到网络上。一旦源节点发送完成，就由网络（网络是互连节点的集合）负责将数据包发送到正确的目的节点。

网络是如何实现这种传输的呢？首先，每当数据包离开源节点时，都没有从源节点到目的节点的预定路径。那么数据包如何找到它的目的地呢？数据包经过的第一个节点具备一些智能，并且建议数据包应该发送到的下一个节点。然后，下一个节点继续将数据包发送到它确认是更接近于目的节点的相邻节点。就这样，将数据包从网络中的一个节点发送到另一个节点，直到到达目的节点。