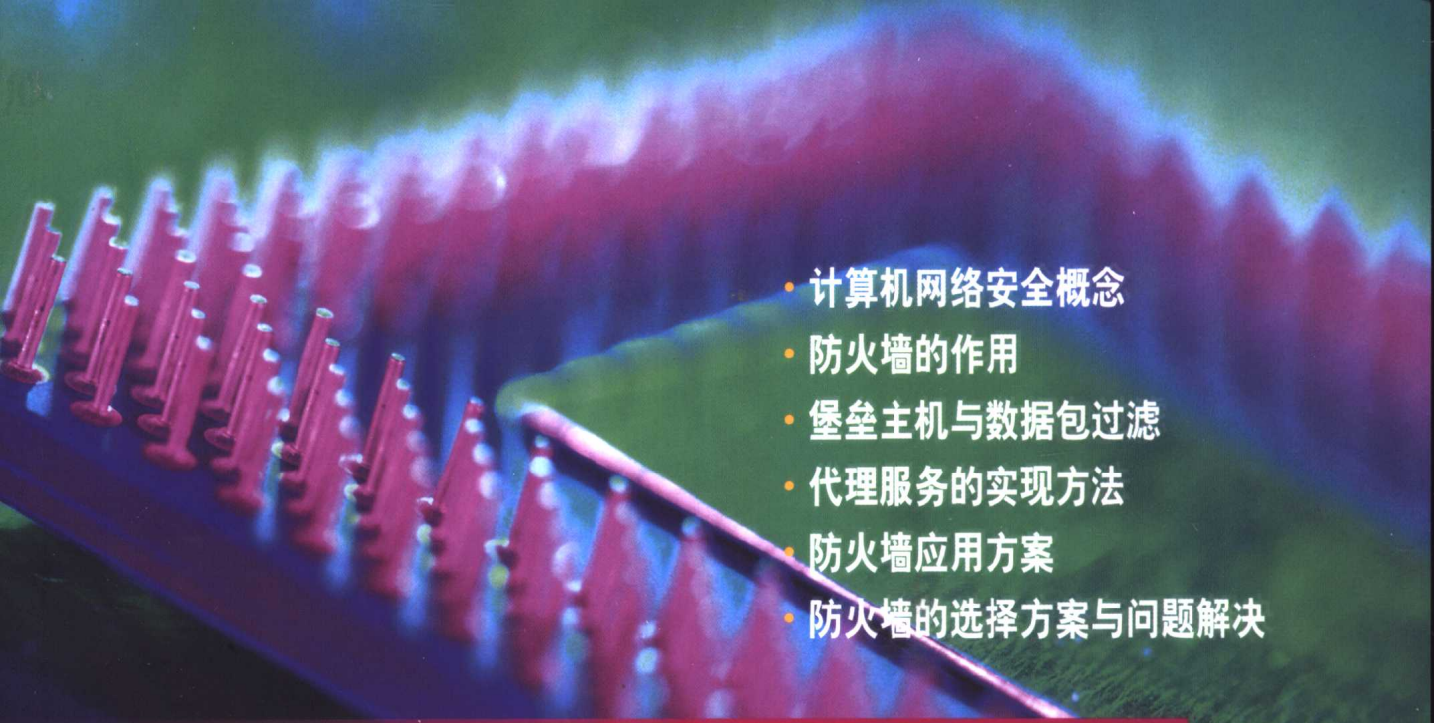

- 计算机网络安全概念
- 防火墙的作用
- 堡垒主机与数据包过滤
- 代理服务的实现方法
- 防火墙应用方案
- 防火墙的选择方案与问题解决

防火墙及其应用技术

FANGHUOQIANG JI QI YINGYONGJISHU

黎连业
张　维
向东明　编著

清华大学出版社

防火墙及其应用技术

黎连业　张维　向东明　编著

清华大学出版社

北　京

内 容 简 介

本书较为详细地介绍了防火墙及其应用技术。内容包括防火墙的概念，防火墙的核心技术，堡垒主机、数据包过滤、代理服务技术，软件防火墙、硬件防火墙、入侵检测技术等，同时对防火墙的选购策略和应用方案也做了较为详细的叙述。

本书叙述清楚，语言通俗易懂。可供网络管理人员、大专院校计算机专业的师生和计算机网络用户阅读参考。

图书在版编目(CIP)数据
防火墙及其应用技术/黎连业，张维，向东明 编著.
—北京：清华大学出版社，2004
ISBN 7-302-08800-4
I. 防… II. ①黎… ②张… ③向… III. 计算机网络—防火墙 IV. TP393.08
中国版本图书馆 CIP 数据核字(2004)第 054577 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：胡伟卷
文稿编辑：刘金喜
封面设计：天福彩文
版式设计：康　博
印 刷 者：北京市通州大中印刷厂
装 订 者：三河市化甲屯小学装订二厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：16.25　**字数**：375 千字
版　　次：2004 年 7 月第 1 版　2004 年 7 月第1 次印刷
书　　号：ISBN 7-302-08800-4/TP·6245
印　　数：1～4000
定　　价：28.00 元

前　言

随着计算机网络技术的发展和因特网的广泛普及，网络安全事故也逐年增多，网络系统的管理责任越来越重大。尤其网上“黑客”、计算机病毒对网络安全的危害，使得人们不得不重视防火墙技术。防火墙是一种行之有效的网络安全机制，它是在网络的内部与外部之间实施安全防范的系统。为使网络管理人员既能对网络进行轻松管理，又对防火墙有一个详尽的了解，能够建立防火墙，提高防火墙与防火墙技术应用水平，为此，中科院计算所(二部)网络研究开发中心培训部组织编写了《防火墙及其应用技术》一书，供从事网络安全的科技人员学习参考，本书由 12 章组成，具体内容如下：

第 1 章介绍计算机网络安全的具体内容及其威胁源，OSI 安全体系结构，网络安全技术等。

第 2 章介绍防火墙的作用、分类、体系结构、组合形式以及防火墙的设计等内容。

第 3 章介绍堡垒主机的种类、其所提供的服务以及建立堡垒主机的方法和需要考虑的因素。

第 4 章介绍数据包过滤所涉及的协议，包过滤的优、缺点，以及包过滤处理内核等。

第 5 章介绍进行代理服务的原因，代理服务的优、缺点，代理服务器的使用方法等。

第 6 章介绍入侵检测的基本内容和体系结构，IDS 的作用与优点以及信息源的有关内容。

第 7 章介绍软件防火墙的有关内容，包括 FireWall-1 的资源要求、体系结构、控制模块、性能和规则语言，以及服务管理器、规则库管理器的使用等。

第 8 章介绍硬件防火墙的产品功能和特点，SonicWALL 防火墙的技术特点及参数等。

第 9 章介绍选择防火墙时需要考虑的关键因素和基本原则，如宏观因素、管理因素、性能因素及抗攻击力因素等。

第 10 章介绍了几个防火墙应用方案，如 SonicWALL 防火墙解决方案、瑞达安全计算机方案和东方龙马防火墙方案等。

第 11 章介绍了配置防火墙时需要注意的问题，联动防火墙，DoS 攻击的有关问题和防火墙的健壮性问题等。

第 12 章介绍子网过滤结构和主机过滤结构的防火墙建筑实例。

本书由浅入深，引导读者了解防火墙、防火墙技术和防火墙设置，能够建立自己的防火墙。

本书由黎连业、张维、番禺职业技术学院的向东明执笔，写作过程中，得到原中科院计算所网络研究开发中心的领导和同行的热情支持和帮助，李淑春、黎娜、王月冬、张维、单银根、陈建华、王兆康、王长富对本书稿提出了许多修改意见并进行了稿件的整理。王刚、刘春阳、滕华、梁艳、刘占全、张静、张洪波、张黎明、顾寿筠等同志为本书的写作提供了许多方便，对上述同志一并表示感谢！

由于作者水平有限，对书中的错误和不当之处，欢迎读者批评、指正。

作　者

目　　录

第1章　计算机网络安全概念

1.1　计算机网络安全性

1.1.1　网络安全性与研究对象

自计算机网络问世以来，网络的安全性一直是人们讨论的话题。随着计算机网络的迅速发展和广泛流行，网络的安全性问题也日趋严重。当资源共享广泛用于政治、军事、经济以及科学的各个领域，网络的用户来自社会各个阶层与部门时，大量在网络中存储和传输的数据就需要保护。这些数据在存储和传输的过程中，都有可能被盗用和篡改。计算机网络十分脆弱，它的安全性遭到破坏就要付出很高的代价，这一点已被美国司法部在1988年进行的一次调查所证实。该项调查报告表明，“当时一次计算机盗窃的平均数额是883279美元。在我国，虽然计算机网络的应用起步较晚，但在金融界也已发生过多起盗窃案，在科技界也发生了用户帐号被盗用，使被盗用户一个月的网络费用损失高达2万余元的情况。因此，对计算机网络安全系统采取措施，鉴别合法用户进行经过授权的操作就显得非常重要。这可以拒绝对敏感数据进行非授权的访问、使用，防止黑客的侵入和计算机病毒的破坏，把计算机网络安全措施落实到实处。

简单地说，网络安全性就是保护用户在网络上的程序、数据及设备免遭别人在非授权情况下使用或访问。

网络安全性的含义实际还包括若干较为复杂的系统管理方面的问题。也就是说，网络安全的目标不仅是保护网络系统的部件、程序、数据免遭他人非法使用和访问，而且也保护企业的权益不受侵犯。

网络安全计划的主要任务是保护系统的数据、程序、设备和网络部件的安全，使其免遭损坏、偷窃或误用，同时也包括需要时使网络提供安全服务。这种网络安全计划的实施可以通过网络操作系统提供的安全工具、系统设计中的冗余以及提供必要的物理屏障阻止非授权人员访问系统部件等手段来完成。

随着科学技术的发展，现代企业解决问题的办法正在变得目的越来越明确，同时越来越依赖于分布计算机网络，使群体人员一起协同有效地工作。另外，对于技术上更加复杂的保护方法的要求也越来越高。网络系统越来越复杂，要想达到预期的安全效果的难度也越来越大。

在实施网络安全计划的同时，其中的一个重要问题就是限制系统的最终用户对系统资源的访问。因为网络安全计划的最终目标是，允许网络用户为使用网络而访问所需的

程序和数据不受任何不必要的限制，使得网络用户能以快速有效的方式访问授权访问的资源。

1.1.2 网络安全的具体内容

网络安全的内容远不只是使用用户识别码和密码，它还包含着广泛的规则和惯例。我们认为：网络的安全性由数据的安全性和通信的安全性两部分组成。数据的安全性是一组程序和功能，用来阻止对数据进行非授权的访问、转移、修改和破坏；通信的安全性是一种保护措施，要求在通信中采用保密安全性、传输安全性、辐射安全性等措施，并且要求对通信安全性信息采用物理安全性措施。通过上述各种措施，可以拒绝非授权的人员在通信中获取有价值的信息。通信安全性的具体定义如下。

- 保密安全性：通过提供技术保密系统以及对密码系统的正确使用来实现。
- 传输安全性：通过采取措施来保护传输不被除密码分析以外的手段截获和利用。
- 辐射安全性：通过采取措施来拒绝非授权的人员获得有价值的信息，而该信息是从密码设备和电信系统的泄露性辐射中截获并分析而得出的。
- 物理安全性：通过采取一切必要的物理措施来保护需要保密的设备、材料和文档，使其不被非授权的人员访问和查看。

通信安全性的分层如图 1-1 所示。

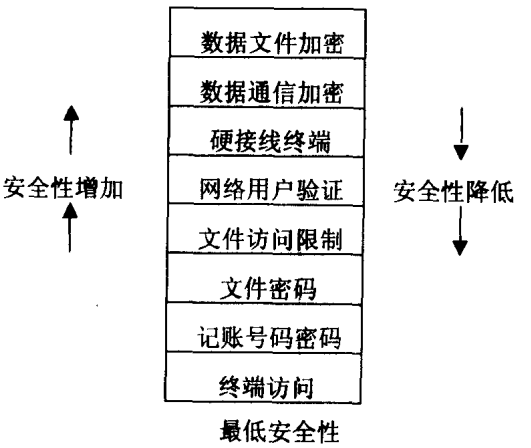

图 1-1 通信安全性的分层

从图 1-1 可知，安全性的技术定义与加密技术有着直接的关系，加密是保护信息最有效的方法。

1.2　网络安全的威胁源

1.2.1　网络安全性面临的威胁

对于网络安全性，我们可以通过甲、乙两个用户在计算机网络上的通信来考察计算机网络面临的威胁，主要有以下几种情况：

(1) 信息泄露

- 当甲通过网络与乙进行通信时，如果不采取任何保密措施，那么其他人就有可能偷看到他们的通信内容。
- 当甲打算把一份文件存放在网络中供乙使用时，如果不采取任何保护措施，那么任何人都可以使用这个文件，而甲并不希望这样做。

(2) 识别

- 对于进入计算机网络系统的用户，系统必须检验其合法性。如果不是系统的合法用户，系统将不给予服务。因此系统要有“身份识别的功能”。
- 当甲和乙用电话进行通信时，甲可以通过声音信号来确认对方是否是乙。但甲与乙用计算机网络进行通信时情况就不同了。若甲的屏幕上显示出“我是乙”时，甲如何确认与他通信的就是乙，而不是冒名顶替者呢？同样，乙又如何确认与他通信的是甲，而不是别人呢？我们把这种现象称为“相互猜疑”。

(3) 假冒

- 甲和乙是网络系统的合法用户，网络为他们提供应有的服务。丙也想获得这些服务，于是丙向系统发出：“我是乙”。系统怎样才能识别出这一服务请求不是由乙发出的，而是假冒的呢？
- 甲收到下述报文：“今晚 7 点在公园大门见。乙”。当甲晚上 7 点去公园大门口时没有见着乙，而是见到了丙，原来报文是丙发的。为了防止假冒报文，报文上一定要有发报人不可伪造的签名。

但对于电子形式的文件，如何签上自己的名字呢？

(4) 篡改

乙给甲发了如下一份报文：“请给丁汇一百元钱。乙”。

报文在转发过程中经过了丙的手。丙就把“丁”改为“丙”。这样甲收到后就成了“请给丙汇一百元钱。乙”。结果是丙而不是丁得到了这一百元钱。当乙得知丁未收到钱时就会去问甲。甲出示有乙签名的报文。乙发现报文被篡改了。

(5) 恶意程序的攻击

除了上述用户之间通信中的信息安全问题以外，网络本身也容易遭受一些恶意程序(rogue program)的攻击。恶意程序种类繁多，对网络安全威胁较大的主要有以下几种：

- 计算机病毒(computer Virus)：一种会“传染”其他程序的程序，“传染”是通过修改其他程序来把自身或其变种复制进去完成的。
- 计算机蠕虫(computer worm)：一种通过网络的通信功能将自身从一个节点发送到另一个节点并启动之的程序。
- 特洛伊木马(Trojan horse)：一种执行超出程序定义之外的程序。如一个编译程序除了执行编译任务以外，还把用户的源程序偷偷复制下来，这种编译程序就是一种特洛伊木马。
- 逻辑炸弹(logic bomb)：一种当运行环境满足某种特定条件时执行某一特殊功能的程序。如一个编译程序，平时运行得很好，但当系统时间为 13 日又是星期五时，它会删除系统中的所有文件，这种程序就是一种逻辑炸弹。

这里所讨论的计算机病毒是狭义的，也有人把所有的恶意程序泛指为计算机病毒。例如 1988 年 10 月的 Morris 病毒入侵美国 Internet 计算机网，舆论说它是“计算机病毒入侵美国 Internet 网”，而计算机安全专家却称之为“Internet 蠕虫事件”。

目前，计算机病毒被分为 3 大类型，即分区病毒、文件病毒和宏病毒。

分布式网络系统的安全威胁分为人为威胁源和物理威胁源两种基本类别。

1.2.2 人为威胁源

人为威胁源有两种，一种是指计算机黑客闯入用户的网络计算机系统，我们把它称为外部危险；一种来自系统的内部，我们把它称为内部危险。

1. 内部危险

网络内部危险包括以下几个方面：

- 设计安全方案过程中，没有考虑员工和公司之间的关系。
- 网络安全需要花费管理人员的精力来维护和实施，造成经费的增加。
- 网络安全威胁主要来自企业内部松懈的、甚至完全不存在的安全措施。
- 用户对限制访问的安全策略有抵触情绪，不遵守安全标准。

要防止内部危险的发生，必须建立一套网络安全标准，规定与网络有关的资源以及每种资源允许的访问权限。另外，应该让用户了解如何正确使用网络资源，并且要制定实施网络安全的措施。

2. 外部危险

网络外部危险包括以下几个方面：

- 窃取机密信息
- 向外部透露敏感信息
- 非法访问网络服务程序和资源
- 干扰网络正常服务

- 故意损害、修改和删除数据
- 窃取或损坏硬件或软件

1.2.3　物理威胁源

网络物理威胁源包括以下内容。

1. 设备故障

设备故障是导致网络数据丢失或无法使用的最常见的原因之一。对网络故障的检测依据是对网络组成部件的监测。轻微故障通常被记录在错误日志中，而严重的设备故障则需要通知网络管理员。如果在网络内配置有适当的冗余系统，就能避免设备故障，降低成本。

2. 物理损害

非法访问网络部件可能导致对系统的物理损害，为防止此类物理损害，需提供足够的安全地域以放置主要的网络设备。

3. 无恢复计划

当发生自然或人为灾难时，必须实施恢复计划。人为地对网络安全进行检查有时也会造成对网络的物理损害。这种危险可能来自网络内部也可能来自外部。

物理保护网络部件安全的程序可以不同，用户可以在网络上安装监视器和报警设备，也可以把网络布线室封闭起来。

1.3　需要多大的安全性

随着 PC 机的普及和大型机构中工作站的普及，信息价值的问题比以往更加引人注目。微型机已被证明是这一问题的催化剂，主要原因是人们希望微型机的工作站能够引用机构数据的一部分子集，并在本地进一步加工、分析和报告。数据库管理员关心数据的完整性，因为数据在使用中经常被修改，因此他不得不了解新的实际情况。如果信息用作一个机构做出决策的基础，那么信息必须是及时的和准确的，这一点比以往更加明显。评估信息的价值，有一部分要看它保证及时性和准确性的花费是多大。

虽然及时性和准确性一直是数据处理人员所追求的目标，然而在过去，常常是在输入处理设备(卡片机等)上生成数据，产生初始报告，检查报告中的错误，改正错误，然后产生最终报告。这一过程常常要进行几天或几个星期。在目前的环境下，终端用户可以控制大部分处理过程，一个文件或一条记录在某一台终端上进行更新，其他某个用户

在另一时刻把该文件或记录下载到一台微机上进行数据处理，并且在一个小时内生成报告。即使完整性已经有技术保证了，而准确性仍然需要人为提供。大型机与微型机在开发与生成报告时间的及时性方面的差别，并不只是微型机易用性技术的结果，也不能看成是大型机系统开发者迟钝的结果。大型机的开发人员要坚持更大程度的整体责任，而不是所谓的终端用户计算，这一点至少是大型机和微型机多年来存在的差别。

在大型机环境中，程序要协调一个机构内部的各种利益，因而常常需要多年的时间才能建立起来，而这样的程序通常不会出现在基于微型机的计算中。此外，许多程序要求在一个大型机环境中运行，这一点直接与安全性考虑有关，因为有些事务在基于微型机的计算中很容易被识别出来，甚至从表面上就被识别出来了。假设在大型机上进行分析，那么大型系统所采取的典型的标准安全性措施可以保证我们不会丢失分析结果，至少不会丢失作为分析基础的数据。如果需要的话，可以复制分析数据，因为标准备份程序总是可以利用的。然而，要想知道微型机上有多少标准备份程序就比较麻烦。一种方法是把大型机看做微型机的外部设备，即把大型机用作备份微型机文件的文件服务器，这一文件服务器既安全，价格也适宜。如果在微型机上生成的文件对机构的决策至关重要，那么这些数据的每一位都和大型机上生成的位同样重要。然而这些数据往往不够安全，并且通常不会给人留下审计的痕迹。

为了回答需要多少安全性这一问题所做的努力，已经催生了多种技术的发展，这些技术对于没有建立适当的安全性所带来的风险，在数量上和质量上做出了估计。一般来说，随着安全性失败风险的增加，并且随着系统价值的增加，进行破坏控制的费用也要增加，这一结论如图 1-2 所示。因此，对于需要多少安全性这一问题的一般回答是，建立足够的安全性程序，使得安全性与修复措施两者的费用最小。一个价值低风险也低的系统，不需要有价值高风险也高的大型系统和相应的安全措施。当然这只是相对的，一个数千美元的系统对于一个公司或一个政府部门来说，可能是无足轻重的，然而它对于一位独立医师、一位作家或者只有一个人的法律事务所来说，却是至关重要的。

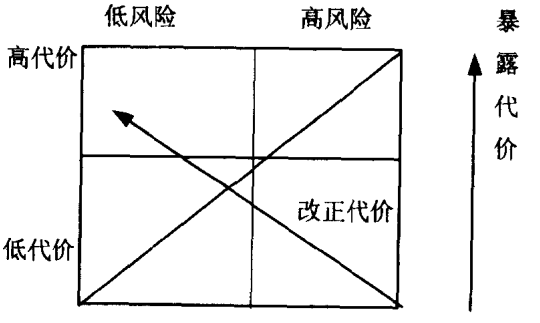

图 1-2　安全性价值与风险的对比

在许多场合，对于一个机构来说，正确估价涉及安全性或缺乏安全性的风险是十分有益的。最早运用数量风险分析的是 Robert Courtney。1977 年，Courtney 在美国 IBM 公司首次提出了这一技术。在这种技术中，风险是以每年可能损失的金额数来定义的，风险可以根据下面的公式来计算：

$R=PE$

其中，R 是风险，P 是每年发生给定次数的安全性威胁的概率，E 是其中每一次破坏所损失的价值。这一公式的难点在于概率要主观指定，并且损失额也常常难以确定。然而这一公式本身十分有用，因为它迫使一个机构中的成员去思考他们的风险损失。

P 并不是一个简单的统计概率估计，这一概率应该看做是损失增殖率(P_L)，它是发生指定风险的年平均率。例如，如果某事件 300 年发生一次，则 P_L 是 0.00333(365/109500，不计算闰年中的闰日)。如果每天发生一次，则 P_L 是 365(365/1)。如果每天发生 100 次，则 P_L 是 36500(365/0.01)。换句话说，P_L 按下式计算：

$$\text{损失增殖率} = (\text{每年的天数}) \Big/ (\text{事件之间相隔的天数})$$

例如，假定一台设备的平均无故障时间是 10000 小时，如果该设备每天工作 24 小时，则两次故障之间相隔的天数是 10000/24=416.67 天，一年 365 天，所以该设备的 P_L 是 365/416.67=0.876。其他某个设备的故障率是每天 2 次，于是每次故障相隔天数是 1/2=0.5 天，所以 P_L=365/0.5=730。某事件每 3 个月(90 天)出现一次事故，则 P_L=365/(90/1)=4.06。还可以用其他技术来估计发生率。但是如果可能的话，这些估计应该以严格的数据为基础，而不要做主观的估计。

估计损失增殖率是很难的，准确地计算损失的代价也很难。损失的代价并不应简单地看做更换的设备的价值，还有许多其他因素要增加由于计算机/通信系统故障造成的损失代价。需要考虑的因素有：

- 由于停机造成的人员生产时间损失。
- 修复故障所需要的人工时间，包括直接的工资及补贴。
- 由于停机所损失的业务价值。
- 使用替代方法的开销(如果能使用替代方法的话)。
- 法律责任的代价。
- 备份与恢复能力的花费，包括年度测试的花费。
- 设备更换的代价，包括订货、运输、安装、调试和启动过程的时间代价。
- 当前资产更换的代价。

上面列举了用于计算“现实的”损失代价的若干因素，这些因素同样也可以用在由于恶意操作而导致的问题中。

对于问题“需要多大的安全性”的回答，要依赖于一个机构可能造成的损失的代价。在安全性上不做任何投资显得太少；大量地投入以至冗余，对于大部分机构来说可能又显得太多。一家汽车组装厂雇佣了几百名工人，每天制造大量汽车，生产流水线由工业自动化网络控制。对于这家工厂来说，它需要非常可靠的安全性以保证正常生产。一家银行显然需要可靠的安全性以防止他人用电子手段私吞资金。在这些情况下，为安全性做出的花费是必需的。

非授权泄露或更改敏感数据会造成多大的破坏，一家机构愿意为它的信息安全付出