21世纪信息安全大系

免费保护你的网络

Secure Your Network for Free

【美】Eric Seagren 著

张骏温　贾卓生　译

科爱传播
KE'AI COMMUNICATIONS

科学出版社

Secure Your Network for Free

免费保护你的网络

〔美〕Eric Seagren 著
张骏温 贾卓生 译

科学出版社
北京

图字：01-2008-3024 号

This is a translated version of
Secure Your Network for Free
Eric Seagren

ISBN-13：978-1-59749-123-5
ISBN-10：1-59749-123-3

图书在版编目(CIP)数据

免费保护你的网络/(美)西格伦（Seagren，E.）著；张骏温，贾卓生译. —北京：科学出版社，2008

（21 世纪信息安全大系）
ISBN 978-7-03-023413-1

Ⅰ. 免… Ⅱ. ①西…②张…③贾… 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（2008）第 181286 号

责任编辑：田慎鹏 霍志国/责任校对：宋玲玲
责任印制：钱玉芬/封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏走印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2009 年 1 月第 一 版 开本：787×1092 1/16
2009 年 1 月第一次印刷 印张：19 1/4
印数：1—4 000 字数：451 000

定价：49.00 元

（如有印装质量问题，我社负责调换）

第一作者

Eric S. Seagren 拥有 CISA，CISSP-ISSAP，SCNP，CCNA，CNE-4，MCP＋I 和 MCSE-NT 证书，有 10 年的计算机行业从业经验。近 8 年来，他为一家“财富”前 100 强的金融领域的公司提供服务。Eric 的计算机职业生涯从接触 Novell 服务器开始，并且在一家休斯敦本地的小公司从事排除一般网络故障的工作。由于他一直在金融服务行业工作，故职位和职责都得到稳步提升，职责包括服务器管理、灾难恢复、业务连续性协调员、千年虫修补、网络脆弱性评估和风险管理。过去几年，他是一名 IT 构建师和风险分析师，设计并评估了安全的、可扩展的冗余网络。

Eric 作为联合作者或技术编辑参与了几本书的编写，包括《强化网络安全》（McGraw-Hill）、《强化网络基础设施》（McGraw-Hill）、《黑客大揭秘：思科网络》（McGraw-Hill）、《配置检测点 NGX VPN-1/FireWall-1》（Syngress）、《防火墙基础》（思科出版社）和《设计开发企业非军事区》（Syngress）。他还获得了美国 Toastmasters 的注册培训经理（CTM）证书。

感谢帮助完成本书的人。首先感谢 Sandra 和 Angela 在整个写作过程中的支持、耐心和理解；感谢 Wes 所给予的质量和一致性方面的建设性的反馈意见；感谢 Holla 提供的最初的思想火花，正是这个火花最终演变成了本书（尤其是第 2 章和第 7 章）；感谢 Moe 在机会出现时的支持。

技术编辑

Wesley J. Noonan（休斯顿，得克萨斯州） 在计算机行业从业已经超过12年，专攻基于Windows的网络和网络基础设施的安全设计和实施。他是NetIQ公司的安全软件产品线上的一名质量工程师。他编写了《强化网络基础设施》（McGraw-Hill）一书，并且是《CISSP培训指南》（Que Publishing）、《强化网络安全》（McGraw-Hill）、《设计开发企业非军事区》（Syngress）和《防火墙基础》（思科出版社）等书的联合作者。他还是《黑客大揭秘：思科网络》（McGraw-Hill）的技术编辑。他是《Redmond》杂志的撰稿人，为该杂志撰写网络基础设施和安全专题，同时为Techtarget.com（http://searchwindowssecurity.techtarget.com/ateAnswers/0,289620,sid45_tax298206,00.html)维护一个叫做“专家咨询”的Windows网络安全版。他还出席了2004年的TechMentor活动。他住在得克萨斯州的休斯顿。

Stephen Watkins（CISSP） 他是有10年以上相关技术经验的信息安全专家，其中8年都投身于安全领域。目前他在维吉尼亚州东南部的Regent大学任信息保险分析师。来Regent之前，他领导一个安全专家组为一个全球规模的政府网络提供深入分析。在过去的8年里，他积累了有关边界安全和多级安全体系结构的专业知识。他的有关Check Point的经验可追溯到1998年FireWall-1 version 3.0b时代。他获得了Old Dominion大学计算机科学专业的学士学位，并且获得了James Madison大学的计算机科学硕士学位，专攻信息安全。他几乎是维吉尼亚海滩的终身居民，他和家人在那里是教堂和当地的少年棒球联盟的活跃分子。

Stephen是第3章的技术编辑。

目　录

Chapter 1

第 1 章
免费安全产品的商业案例

本章主要内容：

- 使用免费安全产品的成本
- 使用免费安全产品节省的费用
- 免费产品与商业产品的比较
- “卖”一个免费产品

- √ 小结
- √ 快速解决方案
- √ 常见问题

引言

你也许正在寻找解决安全问题的省钱的方法，并且想对可用的免费工具有更多了解。本书将介绍一些最好的免费产品。在一些环境中，首倡并实现任何类型的安全措施都会使你陷入麻烦中，即使有最好的计划，也会产生问题。本章将帮助获得所需要的支持，以便实施一个低成本的产品。

无论是对解决方案进行修改并需将修改后的解决方案卖给经理的人，还是需要明白一个特定的免费软件的真正含义的决策者，本章都有助于找到所需的安全产品。本章将讨论免费产品的一些隐性成本，并且阐明这些产品所带来的后果；本章也将说明一个事实：在很多情况下，一个免费包和一个商业产品之间一对一的比较是不合理的。有了所有的信息，就应该能够提出一个解决方案并以一些令人信服的商业数据来支持自己的选择。

使用免费安全产品的成本

至于安全产品，生活中没有什么事是免费的。可能不用为一个安全产品本身付钱，但有关实施产品的费用（这点并不明显）也许就免不了了。很多情况下，安全需要指定哪个产品合适。如果没有一个可用的免费产品，则不得不使用商业产品了。幸运的是，有很多高质量的免费产品可用。后面章节的内容旨在以各种混合等级提供一系列产品。如果未经充分了解和研究就急不可待地实施一个免费产品，则有可能会比购买一个商业产品花费更多。

培训成本

培训成本是实施一个免费产品时最大的支出之一。首先是直接的培训支出（如送某人去听课）。当进行免费软件产品的培训时，选择可能受到限制。在多数情况下，集中于某一主题的培训并不存在（例如，可能找不到一个关于 netfilter 防火墙的课程）。相反，也许能间接地找到适用的培训，如关于普通的 Linux 的使用和管理的课程。

另一项培训成本是资料（如书）。本书只是涉及了某个问题的某点，而除此之外可能还需要该问题的更多信息。例如，如果正实施一个 Snort 入侵检测系统，本书会指导一步步地建立 Snort，但若需要更多信息，则本书就不涉及了。一个覆盖已经实施的特定软件的所有相关领域的小图书馆是值得的投资。

还可能招致培训成本，如培训期间被培训的雇员不可用。此时脱离工作是一项支出，因为你在为一项不可获得的资产付钱。雇员在现场并自行培训的也同样如此。

硬件成本

一个安全设备是一个不需要计算机的设备，并且仅被用于特定的目的，而所有的免费产品都需要一个系统来运行。幸好需求通常是极小的，因此通常可以使用一台旧的 PC。然而，正因为系统的配置是非专用的，所以在使用这样的系统进行连接时，就可

能带来安全风险。系统对资源的需求使得主机几乎不可能再实现其他功能（如 the Snort IDS 日志能力可以很快耗完硬盘空间，不给其他程序留一点空间）。

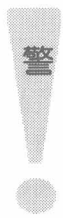
如果没有旧的系统可用，则很多在线的零售商提供价格合理的旧系统。低端 PC 机的很大一部分成本用在操作系统上。很多零售商提供廉价的系统，这些机器要么以 Linux 为操作系统，要么没有安装操作系统。这样可以购买一个相对便宜的较现代的系统，然后把它安装所买来的机器上，这对运行安全工具并提供用户工作站来说是一个可行的选择。

咨询成本

必须谨慎地权衡要把钱花在哪里。培训太少，最终得雇请顾问。实施、配置或安装免费防火墙会比买一个防火墙花费更多。与花 500.00 美元买一个小防火墙相比，所谓的免费很快就不免费了。

虽然那么说，如果需要，还是不要害怕找顾问。与实施某些有专有权的解决方案比起来，高价聘请一个顾问来配置免费产品且保证此配置是基于最佳实践的还是便宜的。一个顾问也可以是一个培训者。可以跟着顾问看他正在做什么，是怎么做的，可以提一些问题并学习为什么那些事情要以那种方式做。通过这种方式，可以让一个博学且有经验的人实施所选定的产品，并且给内部人员提供培训和指导。

如果曾经不得不依赖顾问，可能知道他们不总是“物值其价”。有时他们不像自己说的那么博学。关键是清楚需求是什么并和咨询公司良好地沟通。一个好的顾问可以挽救局面。



警　告

削减咨询预算的时候必须非常谨慎。我看到过试图省钱却以花费更多告终的尝试。在几乎所有的情况下，尽快找一个顾问是最好的做法，从长远来看也是最有效的。如果发现一个喜欢的熟练的有技能的顾问，每月的聘用金也许就是一项好的投资。

无形成本

一个免费产品的所有成本有哪些？对一个初学者而言，是电的消耗。我有一个 Windows 98 系统仅被用作打印服务器。这台机器大约每个月花掉 7 美元的电费。一台专用打印服务器仅花费约 30 美元且不用电，若买这样的打印服务器，5 个月内我就开始省钱。Pentium II 运行 Windows 98 技术上是“免费”的，但是付电费维持运行也不是最划算的选择。一些安全工具不是作为商业产品提供的，而一些是（例如，从一些制造商那里可以得到小的、便宜的且耗电远比标准的桌面 PC 机少的防火墙）。付的电费会不一样。基于电费账单，可以非常准确地计算一台设备会花费什么。

另一个因素是 HVAC［Heating（暖气），Ventilation（通风），Air-Conditioning（空调）］费用。这些基本是环境控制设备。额外的电脑产生额外的热量，这会花掉更多的空调费和电费。如果不能选择一个专用的设备，额外的 HVAC 需求就会是避免不了

的额外费用。相反，在采用更有效的基于设备的产品的情况下，则几乎总是比使用通用的工作站产生的热量少。这也适用于旧计算机与新计算机间的差异。重负荷时要求更多的电力和冷却的新系统常常包含优于旧系统的节能特性。

也有不动产的费用。一台淘汰的全尺寸塔式 PC 比一个新的雪茄烟盒大小的商业设备占据更多空间。也许房间现在有很多空间，但当服务器间变得越来越拥挤时，空间就会成为一个问题。一个键盘、显示器、鼠标（KVM）切换器在空间上节省的费用也许比购买它的成本节省更多。由于服务器包装越来越严密，良好的空气流通和充分的冷却都将被抑制，并且对该系统进行物理访问操作或者维护也会很困难。

考虑到技术支持人员可能不熟悉新的免费产品，由此而产生的低效行为也是免费产品带来的成本。当一名工作人员在新的防火墙上执行一项任务时，不熟悉的防火墙会比熟悉的防火墙花更长的时间。这种低效行为通常只延长了完成一个任务的时间，然而，如果发生停电或业务中断，这一延迟可能导致利润损失或商业损失。规划项目和其他活动时，这些延迟也必须考虑。

免费产品通常是由小型组织或个人制作的。这些产品可以非常好地完成指定的任务，但可能不是很知名。但如果配置免费产品的人离开了或是由于其他原因找不到了，这就可能会产生问题了。如果有一个 PIX 防火墙需要工作，找个人来帮你可能没那么难，但是如果需要一个人来管理一个晦涩的免费产品，找这样的人就很难。这种困难作为一项隐性成本，会通过增加解决问题的延迟时间显示出来，即不得不付给顾问更高的酬金或一些其他的无效行为。

使用免费安全产品节省的费用

以下部分讨论一个免费安全产品是怎么省钱的。首要的节约显而易见：不用为产品付钱。然而，还有其他的好处。这部分提供了关于使用免费软件好处的详细研究。通过评估预期的节约与成本，可以构造一个更实际、准确的关于实施一个免费安全产品能获得什么的全景图。

购买费用

购买费用是使用免费软件时单项最大的成本节约之一。最好的例子就是防火墙。一个小小的 Linksys 或是 Netgear 防火墙价值约在 20～50 美元之间。它们几乎不用电、支持端口转发、执行网络地址转换、可用作动态主机配置协议服务器，且是状态良好的包过滤防火墙。假如使用 Linux 和 netfilter 来运行一个免费的防火墙，则可能员工建立 Linux 防火墙所花费的时间成本会比买一个 Linksys 的花费更多。防火墙是商业产品如何易于得到且负担得起的最好的例子之一。

仍然可以在购买上省钱。有几类产品，尤其是 IDSes、网络分析和报告工具，还有商业虚拟专用网产品的花费数额大的惊人。比较价格的时候，尽可能比较同类产品。把可获得的最贵的“豪华”软件产品用作决策价格是误导人的。免费产品不会有和商业版本一样的特征和性能。以商用产品中认为是必须的那些特性为起点，以这些商用产品的成本为依据，决定免费产品可以节省多少。

维护费用

维护可能是很昂贵的，一年的维护费用为购买价格的 10%很正常。这个价格也是波动的，因为几乎所有的供应商都根据不同的响应时间和服务等级协议确定了不同的支持水平。然而，事实是如果你选择了免费产品并把那 10%花在培训上，可能会有来自员工的非常高的响应度，而确保来自供应商的同等程度响应度和可得性则可能会花掉一大笔。自己的支持人员去办公室或者远程解决这一问题可能会比除最大、信誉最好的供应商外几乎所有的供应商还要快得多。即使供应商可以在 2 小时内到现场，但有时让一个具体的人回复呼叫并对紧急任务做出方案仍需要时间。可能你与员工取得联系所需的时间即使不比这快，至少也一样快。在评估不必购买一份维护合同可节省的成本时，期望的服务水平应该在考虑因素之中。

定制费用

定制能够获得巨大收益还是不合理，这个问题取决于环境。如果购买一个商业产品，可能会发现它没有办法为环境定制。如果能得到某种程度的定制，则它很少是免费的。通常这种服务的小时收费率是相当高的，在真的想要或是需要所期望的功能且愿意付钱来添加它之前，必须明白这点。有了一些免费产品，如果有专门的知识，则这些定制就能负担得起，甚至可以不花钱。然而，并不是所有的免费软件都是可定制的，原因在于它是免费的，但并不总意味着是开源的。开源软件是源代码（例如，使软件运行的程序代码）可以免费获得的软件。当软件是开源的时候，可以下载源代码并把它编辑进核心内容。可以随心所欲地添加或多或少的自定义功能。

很显然，这是一个并不是每个人都需要或有办法利用的优势。取决于考虑的（讨论的）软件包，有些是使用不同的编程语言实现的，因此即使员工知道得足够多，能制定一个程序，他们也可能不知道所要求的特定的编程语言。定制也是进入实施阶段后才知道需要的东西。如果提前知道定制需要，就可以相应地调查权衡费用。总的来说，即使定制免费产品的费用和同等的商业产品的一样，则前者可能达到的定制水平常是（但并不总是）与后者相等或比后者更好。

免费产品与商业产品的比较

当需要做一个正式的决定：是购买一个商业产品还是实施一个免费产品时，有一些与金钱无关的因素要考虑进来。第一个也是首要的因素是，只比较需要的功能。不要把商业产品的豪华版本与免费版本做比较。它们或者特性不一样，或者学习曲线不一样，或者所要求的硬件不一样。最终通过做尽可能最正式和最合理地比较，选择最好的产品。

免费产品的优势

免费产品较之商业产品常有的一个优势是开发速度。开发速度因产品的不同而不同。不是所有的免费产品都有很快的开发周期。开源包常有非常快的开发周期且比相应

的商业产品能更快地解决最新的安全问题。如果要站在前沿，免费软件（尤其是开源软件）也许是比商业产品更好的途径。

前面我们讨论了针对一些免费软件进行定制是节约成本的一个因素。这是因为常常可以自己完成定制，而不用付钱让供应商做。值得一提的是定制本身的优势不仅限于成本节约。这里再强调一次，并不是所有的免费软件都可以定制。有时候一个特定类别里最好的软件使用了封闭的代码，因而没有办法执行任何定制。但是开源运动最大的优势之一就是每个人都有编辑、定制和改进软件的自由。

免费产品的一个潜在的优势是实施的速度（这个速度有别于开发速度）。当我提到免费软件的实施速度，我是指装载该软件并让它工作所需要的时间。这不只包括安装，有时还包括重大购买时的繁文缛节。例如，假如正尝试建立一个将有利于组织的商业合作关系。这里时间是重要因素，合作关系越快建立越好。合作关系涉及网络连接以促进信息交换。检查了网络连接方案后，潜在伙伴开始犹豫不决，因为方案中缺乏充分的防火墙保护。也许当前的因特网连接用一个消费者级的家用路由器或是防火墙进行过滤，而现在却需要一个单独的非军事化区 DMZ，这个 DMZ 要有一些高级的地址转换规则和较好的日志。可以联系一家供应商并等待回应、得到一个报价并传给经理征得同意。经理同意购买计划后，把它交给财务部，他们购买并安排运输。一旦新的防火墙到了，必须安装、配置这个新的防火墙，然后测试。相反一种更快的方法是从储藏室找台旧的 PC，下载并在这个旧的 PC 上安装 Linux，配置防火墙。如果环境允许这样做，则实施免费软件会相当快。然而在对允许的供应商、许可软硬件等有限制的环境中，获得一个免费产品的许可会比获得一个商业产品更难更费时间。最终，环境将会证明实施速度是否真正是一个优势。

人们可能认为所有的免费软件都是由一些学校毕业的孩子制作的，不稳定且缺乏类似商业软件开发项目的质量管理。有时这当然是对的，有时却并不是这样。事实上，大的、建立良好的开源项目有上百的程序员评审、修订、详察、修改代码。几乎没有商业公司会把相同数量的资源放到一个单独的软件产品中。这就意味着在很多情况下，正在获得的免费软件比对应的商业软件经过了更多的同行评审和测试。这并不总是正确的，很多情况下免费软件几乎没有质量管理，而真正进行测试的是用户。根本上讲，这意味着免费软件的质量会有很多变数。为了减少正在实施满是 bug 的软件的情况，需要投入大量的业余精力。如果坚持使用成熟的产品，当然会提高实施成功的机会。避免使用改变了主要体系结构的新发布版软件也会有所帮助。如果正使用的某个产品的当前发布版新增了对最新芯片组的支持，则在实施该发布版之前多做些测试是明智的。关于免费软件的优点的优秀的长篇文章参阅 www. dwheeler. com/oss _ fs _ why. html。事实上，一些免费产品不适合充当任何类型的关键角色，其他一些则可以。最后，并不是所有的免费软件都是“廉价”软件，部分免费产品有很高的技术含量。

免费产品的劣势

在生产环境中，实施一个免费产品惟一最大的缺点就是支持，或是缺乏支持。从因特网上免费下载一些东西时，通常没有电话号码可用来寻求帮助。有时高质量的文档可

以使这一问题得到部分解决，某些情况下，可以在为数众多的在线用户论坛上提问，并且得到软件包制作者或是其他用户的帮助。另一方面，高质量的文档非常稀少。很多免费工具软件（utilities）非常缺乏文档。这个问题是管理中最需关注的问题之一。一般而言，安全软件的关键性越大，实施一个有很少支持的产品时就应该越谨慎。如果你是一家依赖互联网的公司，比起其他在店面里赚钱且只用互联网来冲浪的公司，在实施一个免费的 Linux 防火墙之前，需要内部技术人员具有更高级别的专门知识。这并不是说免费软件没有充分的支持或是不应该使用免费产品来满足关键需求，只是说应该在认真考虑和计划后有意这样去做。

免费安全产品的管理能力通常没有商业产品的那么健壮，需要根据所使用的特定产品来决定这是否是一个真正需要考虑的因素。对于免费的入侵检测系统、反病毒和反间谍软件，管理能力的有或无常常更重要，这是因为这些产品都需要频繁地更新以便保持价值并有效地工作。一个企业级的反病毒程序将会围绕签名提供很多更新的控制和特征，如什么时候和如何执行更新，以及侦测到一个病毒时该如何处理。免费产品通常有更多局限，常需要手动扫描或更新程序，并且可能必须通过一个交互程序人工响应一个主动侦测，而不是自动响应。

有时免费产品还缺乏的另一个领域是报告。一些免费产品提供卓越的报告，其他很多免费产品则很少或没有提供报告的能力。在很多情况下，使用免费工具软件自己手动配置一些类型的报告，但即使能生成一些自动化的日志或报告，它也不会如一个本来就支持这些功能的商业产品那么简单或快捷。当考虑免费产品的报告能力时，你不仅要考虑想要的日志能力，还要考虑需要的日志能力。很多情况下，如果你在一个高度受管制的行业，如银行业或是卫生保健，是否有丰富的日志能力是导致是否购买商业软件的关键因素。如果需要通过审核，在制定出一个关于产品的战略决策之前，就要研究能仔细地生成的审核记录。

前面粗略地谈到免费产品常常是不知名的这一事实，以及如何转变成诸如咨询费用这样的隐性成本。这一隐性成本可能不限于咨询费用。如果你正要雇用一名新职员，并规定他们需要熟悉思科的设备，毋庸置疑，能很快找到你要的人，但如果规定他们要熟悉一些几乎无人知道的已经用过的免费产品，则会非常难。这并不是说他们不能被培训，只是这又会引来培训有关的成本和缺点。熟悉一个产品（因其无名）也能使实施一个产品比实施一种广为人知的技术所花的时间更长。实施（完成）速度在这里是作为潜在的资产被提到的，但是，如果找不到一个了解免费产品的人，这很容易就会变成债务。最终，使用行业标准产品比使用不广泛的产品有优势。

测评单个产品

研究一个免费产品时，需要决定该产品是不是最好的产品，做这个决定时有很多因素要考虑。下列列表简要概述了所需要的步骤，这些步骤决定一个免费产品对你而言是否是最好的。

（1）识别可供选择的产品

知道存在哪些可选择的免费产品，这可能是整个测评过程中最难的部分。希望本书会帮助你，除此之外在在线网站也会帮助找到免费软件。拥有开源软件的最大网站之一