GOTOP

MVP
Microsoft
Most Valuable
Professional

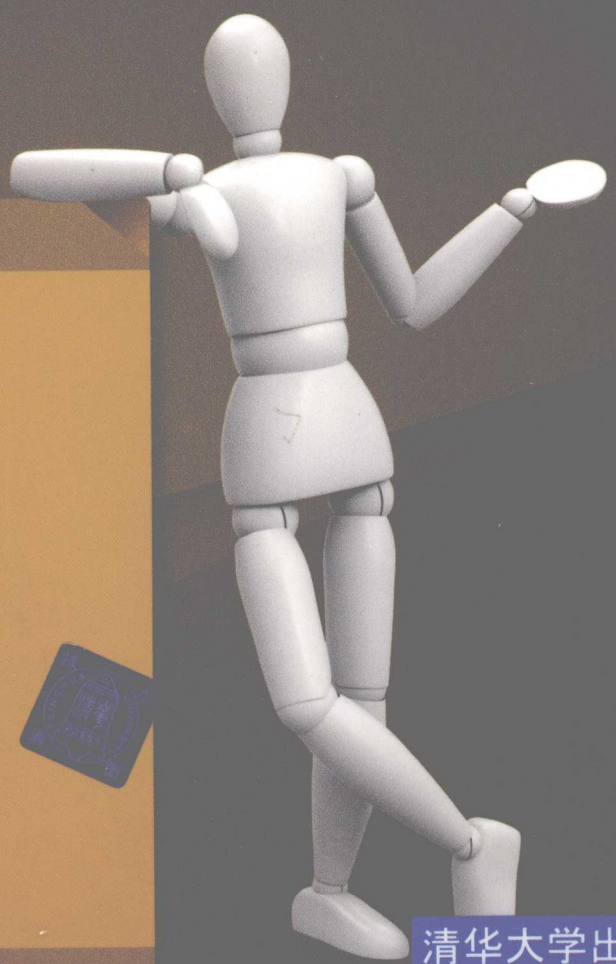
Microsoft®

ISA Server 2006

企业级防火墙 实战彻底攻略

（适用于ISA Server 2006/2004版本）

顾武雄 编著



- ISA Server各种用户端类型的部署指导
- 企业各类服务器的安全管理与彻底防御
- 整合SharePoint网站安全防护应用
- 企业版ISA Server进阶应用指南
- 整合Winfrasoft VPN-Q安全隔离控管
- 整合硬件防火墙VPN网络的设计
- 整合智能卡与动态密码的进阶应用
- 无线局域网络最高安全规划指南
- 阐述Forefront Security整体解决方案

清华大学出版社

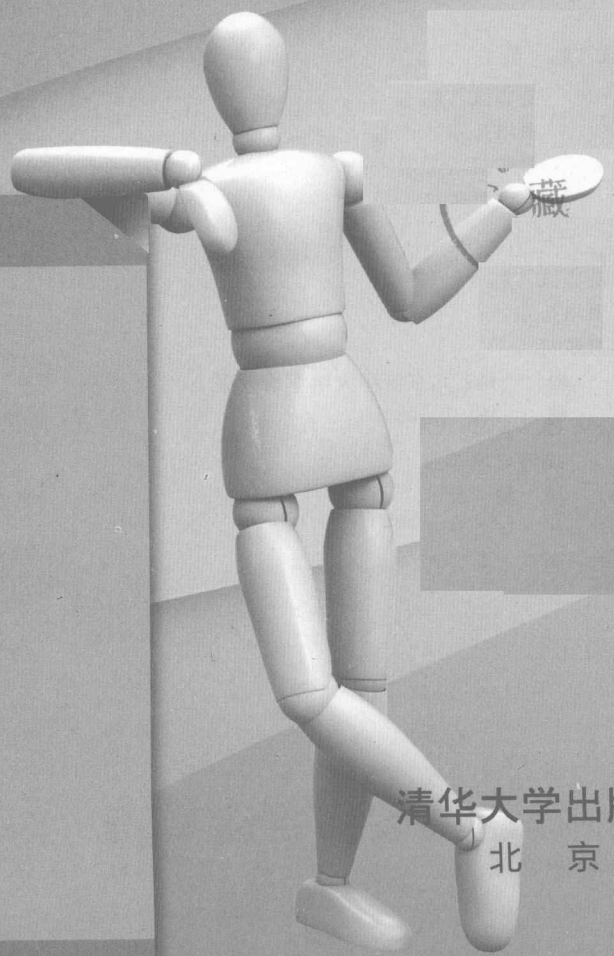
Microsoft®

ISA Server 2006

企业级防火墙 实战彻底攻略

（适用于ISA Server 2006/2004版本）

顾武雄 编著



清华大学出版社
北 京

图书在版编目（CIP）数据

Microsoft ISA Server 2006 企业级防火墙实战彻底攻略/顾武雄编著.
-北京：清华大学出版社，2008.11

ISBN 978-7-302-18797-4

I. M… II. 顾… III. 计算机网络-防火墙-应用软件，ISA Server 2006　IV. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 165489 号

责任编辑：夏非彼　陈　晨
装帧设计：图格新知
责任校对：贾淑媛
责任印制：何　芊
出版发行：清华大学出版社　　地　　址：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　邮　　编：100084
社　总　机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市昌平环球印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：190×260　印　张：29.25　字　数：711 千字
版　　次：2008 年 11 月第 1 版　　印　　次：2008 年 11 月第1次印刷
印　　数：1～4000
定　　价：56.00 元

内 容 简 介

本书为当今Microsoft ISA Server资深专家(MVP)顾武雄先生的精心力作，内容中以Microsoft Windows系统为操作平台，以新一代的软件防火墙技术——ISA Server 2006/2004为工具，结合从实际工作中挑选的代表性案例，向读者提供全方位的企业防火墙架设策略。

全书共分5章，前4章分别介绍企业信息安全基础概念、ISA Server 2006基础管理、企业因特网服务器安全防御、ISA Server 高级管理，这些内容适合第一次接触ISA Server的2006/2004版用户；第5章“企业网络信息安全加强防御”，主要介绍ISA Server 2006的各项新功能应用、ISA Server 整合硬件防火墙的VPN网络设计、整合Winfrasoft 的VPN-Q隔离控管功能，以及无线网络的安全部署、数字签名、邮件加密等的应用，适合正在使用ISA Server 2006且对ISA Server比较熟悉的用户。

本书向读者介绍了ISA Server 2006、ISA Server 2004最精华的实战内容，是企业信息安全人士必备用书！

改编者的话

ISA Server 2006 是微软出品的一款非常优秀的企业级路由防火墙，目前在国内众多企业中应用十分广泛。ISA Server 2006 以其良好的管理界面，灵活的多网络支持，易于使用且高度集成的虚拟专用网络配置，可扩展的用户身份验证模型，全新的服务器发布规则，深层次的 HTTP 协议检查等功能赢得了使用者的一致好评。目前 ISA Server 2006 已成为国内中小企业软件防火墙的首选产品。

很多 ISA 使用者很希望有一本好书能帮助他们解决学习和使用 ISA 时所遇到的诸多难题，但国内图书市场中缺少系统介绍 ISA Server 2006 工具书的这个现状让他们失望过很长时间。但现在，我终于可以恭喜他们了！台湾资深 IT 专家顾武雄先生为我们带来了他的大作《ISA Server 2006 企业级防火墙彻底攻略》。这本书既能由浅入深地为初学者提供学习指引，又能系统深入地介绍 ISA Server 2006 高级特性。难能可贵的是，作者还利用自己在安全领域内丰富的实战经验，带领读者将 ISA Server 2006 和 Rsa SecurID、智能卡、无线安全网络等诸多领域进行了广泛的横向联系，极大地拓展了读者的视野，提升了读者构建安全网络架构时的想象力。

最后要感谢出版社图格新知公司的夏老师让我有机会参与将这本书的繁体中文版改为简体中文版的工作。希望通过我的工作，读者能更好地从书中汲取养分，学到内容精义。由于本人能力有限，疏漏之处烦请读者不吝指正。

岳　雷

2008 年 9 月

序

近些年，很多企业的IT部门都在寻找符合自身信息安全管理需求的解决方案。寻找过程中，一般都会考虑涉及面很宽的许多内容，包括远程访问安全、内部网络检查管理、入侵检测管理、即时通信管理、垃圾邮件筛选、数据库安全、商业机密外泄的管理控制机制等。由此可见，当今社会除了应验“商场如战场”这句名言之外，同时也拜信息科技所赐，形成了信息战的局面。只要谁能够成功防守企业信息安全无忧，同时又能够迅速创新，并掌握大量的信息，该企业迅速成长为顶尖企业便指日可待了！

然而，谈到企业信息安全的整体规划，对于许多IT人员来说似乎范围太大了一些，不知从何着手。总的来说，为了防御来自因特网的安全威胁，必须在内部网络与因特网之间架设一道坚固的安全防线，即防火墙。这是一切安全设施的基础，因为这道防线搭配守卫就可以有效地管理一切人、事、物的往来。

本书重点介绍的ISA Server，便是巩固企业信息安全的最重要的基础设施，若能够与书中介绍的其他安全设施、加密机制、隔离措施等进一步整合，相信就算面对再大的信息安全威胁，也能够稳如泰山。

由于ISA Server 2006采用了与ISA Server 2004相同的操作界面，因此笔者在整理此书的内容时，在许多非ISA Server 2006新增功能的使用方面，皆以ISA Server 2004作为范例，因为二者最多在操作界面上有个别选项只是名称略有不同而已。例如原有的“发布服务器”功能在新版中变成了“发行服务器”，所以没有给出2006与2004的对照操作界面。

对于ISA Server 2006的全新应用，比如针对Exchange Server 2007的远程联网发行设置、SharePoint网站的发行设置、远程网站的负载平衡容错机制等，都可以在本书的相关章节找到。

因此，如果你是第一次接触ISA Server，并且目前正在使用ISA Server 2004的SP2版本，建议你可以先阅读第1～4章。相反，如果你已经熟悉ISA Server 2004的应用，并且目前已经开始使用ISA Server 2006了，则建议您直接阅读第5章的相关内容，因为在该章的内容中除了可以学习ISA Server 2006的各项新功能应用、ISA Server整合硬件防火墙VPN网络、整合Winfrasoft的VPN-Q隔离控管功能之外，还可以学习到有关无线网络的安全部署、数字签名、邮件加密等的应用。

各位在学习中不论遇到任何问题，都可以登录 IT 开封府部落格：

http://tw.myblog.yahoo.com/chivalrous_ku

与本书作者探讨解决方案。

顾武雄 Jovi Ku

2008 年 9 月 8 日

目　录

第 1 章

企业信息安全基础概念

在一个企业 e 化的过程中，最重要的一项基础建设是什么？答案就是“信息安全”。对于一个漠视信息安全规划的企业来说，在任何系统上架设的应用环境到头来终究会面临安全方面的重重危机。因此在企业信息安全的整体规划上，需要从正确的信息安全基础观念开始。在本章内容中，您将会学习到最清晰易懂的安全观念。此外，针对企业网络安全的基础设施——防火墙，在本章中也将为您剖析软硬件防火墙之间的差异，以及 Microsoft ISA Server 2006 与 2004 版本的整体技术概述。

1-1 信息安全的重要观念

网络科技的兴盛同时也燃起了企业对于信息安全的重视，其主要原因是它提升了企业间的往来效率，加速了彼此间的数据传递速度，如此也让人与人之间以及公司与公司间的有价信息面临了极大的安全挑战。

信息安全究竟有多么重要呢？根据 2004 年 CSI/FBI 计算机犯罪与安全调查的数据显示，以 2003 年为例，单单遭受病毒危害而造成的财物损失案例就有 254 件，至于所损失的总金额更高达 27382340 美元。事实上那样的损失还不是最糟糕的，因为由于网络安全架设上的疏忽，而遭受 DoS 攻击的案例也有 111 件，虽然发生的总件数远低于病毒所造成的危害，但总损失的金额却高达 65643300 美元。我们把这两部分所造成的损失加起来，是非常可观的，由此可见，在享用信息科技所带来便利的同时，信息安全的重视也千万别忽略了，一旦您漠视了它，下一个遭受危害而损失惨重的名单中，可能就有您的企业名称。

至于企业信息安全的整体规划，可从下列两个层面来着手：

- **技术层面**：此部分主要是通过 IT 人员的专业能力，将现今市场上有效的网络安全产品集成于企业内部，例如防火墙、防病毒系统、入侵防御系统（IDS 或 IDP）、加密证书系统等。
- **管理层面**：此部分则是重视人的管理部分，通过完善而有效的信息安全政策来管理企业内部信息的安全，根据统计，由于内部网络访问的滥用以及未经授权验证而访问所造成损失的比例，分别有 80%以及 71%之多。

完成了上述两个层面的规划之后，别忘了一定要让您企业网络的信息环境，达到机密性（Confidentiality）、完整性（Integrity）以及可用性（Availability）的三大诉求。

1-1-1 架设防火墙的目的

- **过滤进出企业的网络数据包**：进出于企业网络中的数据包传递，都必须得使用不同的通信协议，以及通信端口来进行彼此的沟通，因此只要经过防火墙的网关管控，便可以只让所需要的通信端口开启，以此维持企业整体网络的基本安全。
- **记录进出企业网络的连接行为**：在防火墙所承担的工作内容中，除了要能够进行网关的安全管理之外，还必须得记录每一个进出的旅客行为，以便于管理员在事后可以进行安全的连接访问分析，如此才能够将一些可能危害内部网络安全的旅客名单一一封锁。
- **避免主机直接暴露在因特网上**：通过防火墙的架设，可以在内部的虚拟网络与因特网上的其他连接计算机之间，采取最重要也是最基本的隔离措施，如此一来即使遭受攻击时也不会在第一时间直接受害，但是这只是第一层的防护而已，还必须得依赖防火墙本身的细节防护机制来构建多道的防护措施。
- **防范日益猖獗的网络型病毒**：如今的病毒与十几年前的病毒类型相比，可以说是

大大的不同，我想应该说是“技术规格”上的落差甚大！这当然也是网络科技发展迅速的因素而导致，怎么说呢？以往的病毒是靠磁盘的互相传递访问而感染，病毒传播的速度很慢，因此进行危机处理时的缓冲时间也相对的比较长，可是如今大多数的病毒都是通过网络系统的漏洞，或通信端口的开启来进行迅速蔓延，所以，在目前的企业信息网络环境中，防火墙早已成为最基本的重要配备了，在此奉劝各位随时检查自家的门窗是否已安然关好。

1-1-2　防火墙无法防范的来源

- **新的黑客攻击手法**：黑客的攻击行为与所用的工具软件是日新月异，五年前的防火墙在防护功能上的设计较为简陋，因此要用来和现今各类新型的病毒抗衡是会力不从心的，因为撰写病毒程序的人，不单单只是挑战各类系统的漏洞所在，更要考虑的是如何无声无息的通过前面那道墙的阻碍。
- **内部人为的祸害**：正所谓家贼难防，在这里便是说许多网络管理者，往往可以通过许许多多的精密仪器来监测外来的攻击或窃取，但却时常忽略了内部自己人的管理问题，因此可别忘了！不要依赖信息科技设施来帮您打理一切事务。
- **不同的物理线路**：如今有许多的企业内部可能都有两条以上的物理线路，根据调查，除了是线路的租金费用低廉之外，主要都是为了针对不同的用途来管控带宽流量与访问安全的问题，当然也还有少部分的公司在使用传统的调制解调器（Modem），除了提供传真共享以外，有些则是为了可以通过外部拨号连接来进行数据的传递或远程控制，因此如果网络病毒或黑客的入侵并不是走正门进来，那它也只能说无能为力了。

1-1-3　防病毒系统无法防范的来源

- **第一时间感染的新病毒**：由于现今网络使用的普及，导致病毒的传播方式已由过去磁盘感染的方式，转为通过网络进行爆发式传播，因此新病毒从产生到传播于整个国家或全世界，可以说是迅雷不及掩耳，让我们这些爱好和平的无辜用户想避都避不掉，虽然说在全世界有许多的防病毒厂商，通常在病毒发作的第一时间内都会发布关于病毒危害的新闻稿、网页公布、电子邮件等，来让用户能够赶紧上网去进行病毒码的更新或系统的安全更新等，可是为何还是会有一大串数也数不清的受害者呢？其实原因很简单，就是因为多数的用户都没有阅读这些信息的习惯，同时警觉性不够，或者是即使知道了也不会认为下一个中标的会是他，其次则是病毒的传播速度太快，而防病毒厂商的动作太慢，这就好像电影中的情节一般，往往在一位杀人犯已经干掉一群被害人之后，警察才会到现场来一一收尸，像这样的类似剧情套用到现今的信息市场中，可以说是最贴切不过了。
- **管理者的疏忽**：在公司这样的信息环境中，无论规模大小与否，信息安全的巩固全部是操作在 IT 人员的手中，而不是在出钱的老板身上，说到这里笔者可能会遭受许多 IT 人员的反驳，原因是老板不肯花钱什么事也做不了啊！不过话说回来，