

GOTOP



Microsoft®

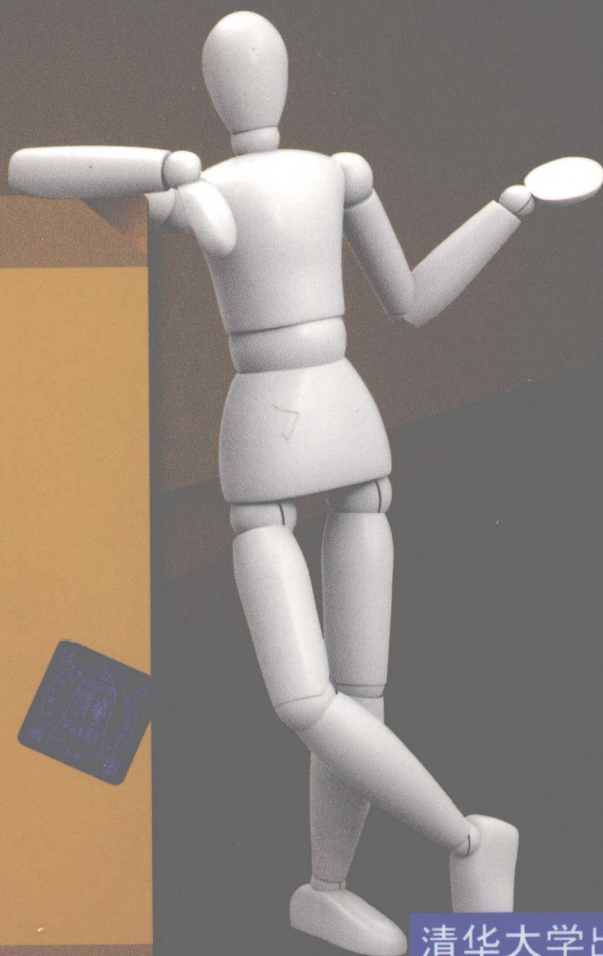
ISA Server 2006

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Winfrisoft 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

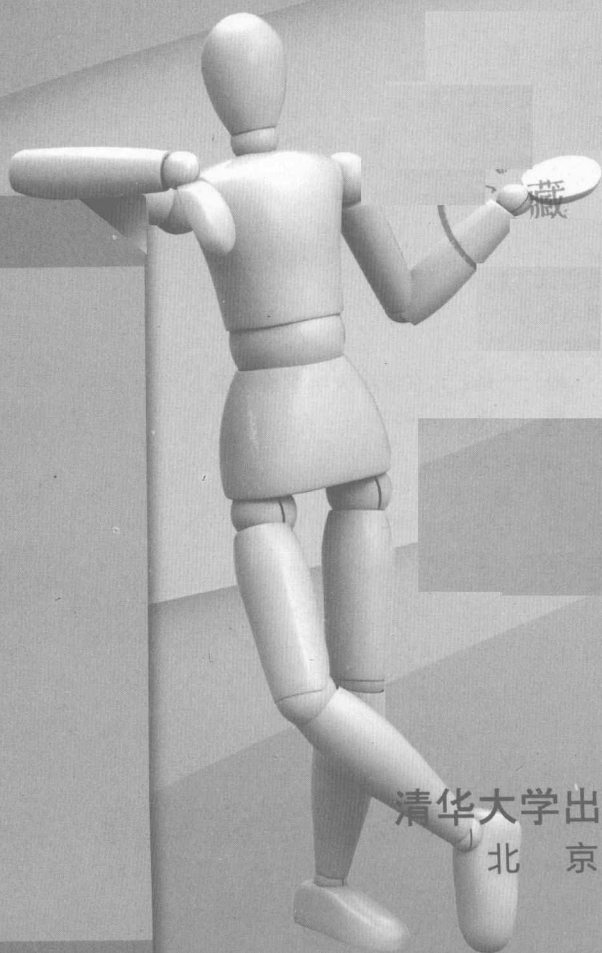
Microsoft®

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

本书版权登记号: 图字: 01-2008-4100

本书为经台湾碁峰咨询股份有限公司独家授权发行的中文简体字版本。本书中文简体字版在中国大陆的专有出版权属清华大学出版社所有。在没有得到本书原版出版者和本书出版者书面许可时,任何单位和个人不得擅自摘录、复制本书的一部分或全部以任何方式(包括资料和出版物)进行传播。本书原版版权属碁峰资讯股份有限公司。版权所有,侵权必究。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话: 010-62782989 13701121933

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

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话: (010)62770177 转 3103 产品编号: 029779-01

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护、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	1
1-1 信息安全的重要观念	2
1-1-1 架设防火墙的目的	2
1-1-2 防火墙无法防范的来源	3
1-1-3 防病毒系统无法防范的来源	3
1-2 构建安全的 e 化环境	4
1-2-1 影响企业信息安全的六大因素	4
1-2-2 防范人为危害的七大建议	5
1-3 软硬件防火墙的简介	8
1-3-1 防火墙采购原则	8
1-3-2 软硬件防火墙的比较	9
1-4 ISA Server 2006 的功能特色	10
1-4-1 ISA Server 2006 与 ISA Server 2004 相同的管理功能	11
1-4-2 ISA Server 2004 Service Pack 2 附加功能	13
1-4-3 ISA Server 2006 全新功能一览	17
1-4-4 ISA Server 2006 的 Web 侦听器设置	19
1-4-5 ISA Server 2006 的验证方法	20
1-4-6 ISA Server 2006 的安全验证机制	21
1-5 各类防火墙架构介绍	30
1-5-1 防火墙的分类	30
1-5-2 防火墙的架构特点	31
1-5-3 防火墙的整体规划架构建议	34
1-6 缓存机制的架构应用介绍	34
1-6-1 ISA Server 缓存工作方式	35
1-6-2 ISA Server 2006 缓存工作类型	36

第 2 章	ISA Server 2006 基础管理	38
2-1	安装前的考虑与准备工作	39
2-1-1	安装前的考虑	39
2-1-2	基本系统需求	39
2-2	开始安装 ISA Server 2006	40
2-3	各类客户端的部署说明	47
2-3-1	各类客户端的使用时机	47
2-3-2	SecureNAT 客户端安装设置	48
2-3-3	Web 代理客户端安装	49
2-3-4	防火墙客户端安装	54
2-4	访问策略的控制技巧	57
2-4-1	自定义防火墙访问规则	57
2-4-2	访问外部网站的高级控制	64
2-4-3	HTTP、FTP 数据包过滤设置	67
2-5	监控 ISA Server 的状态	77
2-5-1	认识 ISA Server 2006 的“监视”选项	78
2-5-2	系统管理委派向导的使用	83
第 3 章	企业因特网服务器安全防护	85
3-1	黑客攻击手法面面观	86
3-1-1	黑客攻击思维模式	86
3-1-2	常见黑客攻击手法	89
3-2	Web 服务器的防御措施	92
3-2-1	关于公司网站架设的建议	92
3-2-2	网站发布策略	93
3-2-3	链接转换	100
3-2-4	HTTP 筛选器设置	103
3-3	FTP 服务器的防御措施	104
3-4	Exchange Server 安全发布管理	110
3-4-1	ISA Server 2006 发布企业 Exchange Server	110

3-4-2	ISA Server 2004 SP2 发布企业 Exchange Server	115
3-5	终端服务器的防御措施	127
3-6	域名服务器的防御措施	133
第 4 章	ISA Server 高级管理	139
4-1	企业 VPN 网络的架设	140
4-1-1	架设企业 VPN 网络的 3 种方式	140
4-1-2	VPN 环境架构模拟实战	141
4-2	企业 VPN 网络客户隔离控制	164
4-2-1	客户端隔离控制简介	164
4-2-2	VPN Server 与 RADIUS 的集成配置	168
4-2-3	Remote Access Quarantine Agent Service 的安装	171
4-2-4	添加远程访问规则	173
4-2-5	配置 VPN 客户端隔离访问策略	176
4-2-6	连接管理器系统管理工具包 (CMAK) 的使用	180
4-2-7	ISA Server 2004 VPN 隔离控制应用	189
4-3	DMZ 网络的架设	192
4-3-1	DMZ 网络的典型架构	192
4-3-2	使用 DMZ 网络模板架设 DMZ 网络	192
4-4	集成 RSA SecurID 应用安全指南	198
4-4-1	开始配置 RSA ACE/Server	200
4-4-2	配置 RADIUS 服务器	206
4-4-3	配置 ISA Server 的 VPN 网络	208
4-4-4	VPN 客户端连接配置与登录	211
4-4-5	ISA Server 集成企业网站与 RSA SecurID 侦听配置	215
4-4-6	使用 RSA SecurID 客户端进行网站登录	217
4-4-7	小结	218
4-5	构建最安全的数据传递与访问管道	218
4-5-1	安装证书服务	219
4-5-2	SSL 安全连接架设范例	221
4-5-3	ISA Server 配置说明	229



4-5-4	CA 证书服务与 EFS 的集成应用	232
4-6	报告的使用与解读	235
4-6-1	创建和配置报告任务	235
4-6-2	报告的解读	239
4-7	警报的使用与解读	243
4-8	备份与还原的规划使用	251
4-9	日志文件与 SQL Server 的集成应用	255
4-9-1	配置日志文件数据库	255
4-9-2	用 SQL Serve 的 Web 助手向导自定义报表	265
4-9-3	ISA Server 日志文件分析工具	272
4-10	缓存的高级配置	274
4-10-1	架构单一网卡的缓存服务器	274
4-10-2	建立防火墙新访问规则	278
4-10-3	缓存磁盘驱动器与缓存配置	283
4-10-4	自定义缓存规则配置	285
4-10-5	配置计划缓存规则	288
4-10-6	链式缓存配置说明	293
第 5 章	企业网络信息安全加强防御	295
5-1	ISA Server 企业版高级应用实务	296
5-1-1	ISA Server 企业版安装说明	298
5-1-2	企业策略的管理	301
5-1-3	分布式缓存的使用	302
5-1-4	客户端自动发现设置	304
5-1-5	网络负载均衡的使用	306
5-1-6	小结	308
5-2	ISA Server 2006 集成 Antigen 部署安全环境	309
5-2-1	ISA Server 2006 设置说明	310
5-2-2	IIS SMTP 服务设置说明	313
5-2-3	Antigen for SMTP Gateways 安装设置说明	314
5-2-4	垃圾邮件筛选管理	315

5-2-5	文件筛选管理	316
5-2-6	Antigen Enterprise Manager 集中控制	317
5-2-7	集成 MOM 监控 Antigen 运行	318
5-2-8	小结	318
5-3	ISA Server 2006 集成 SharePoint 安全防护应用	319
5-3-1	SharePoint 2003 新特性	319
5-3-2	反向 Proxy 连接访问工作原理	321
5-3-3	完成 SharePoint 网站备用访问映射 (AAM) 设置	321
5-3-4	网站自动转换说明	325
5-3-5	发布 SharePoint 服务器阵列	326
5-3-6	远程单一登录的集成应用	330
5-3-7	证书管理与验证委派的使用	331
5-3-8	验证委派的使用	333
5-3-9	小结	334
5-4	ISA Server 2006 分支机构 VPN 网络架设	334
5-4-1	ISA Server 2006 在分公司网络集成管理的新特色	334
5-4-2	VPN 网络架设操作实例说明	335
5-4-3	开始建立台北总公司与高雄分公司的 VPN 网络连接	337
5-4-4	远程安装设置高雄分公司的 ISA Server 2006 企业版	338
5-4-5	针对 ISA Server 2006 KH 阵列建立一个访问规则	341
5-4-6	小结	342
5-5	深入 ISA Server 2006 集成 Winfrasoft VPN 隔离控制	342
5-5-1	VPN-Q 2006 功能简介	343
5-5-2	完成 ISA Server 2006 VPN 网络的启用	343
5-5-3	完成 VPN-Q 2006 的安装与基础设置	346
5-5-4	VPN-Q 2006 安装后的高级组件配置	348
5-5-5	开始 VPN 客户端连接检查测试	350
5-5-6	VPN-Q 隔离策略的集中控制方法	353
5-5-7	小结	356
5-6	ISA Server 集成硬件防火墙 VPN 实务	357
5-6-1	架设 Windows Server 2003 LAN Routing	358

5-6-2	新增分公司 VPN 网络设置	360
5-6-3	新增分公司 VPN 网络规则	362
5-6-4	新增分公司与总公司防火墙策略	363
5-6-5	开始设置分公司 PIX 506 组件	364
5-6-6	监看 IPSec VPN 网络即时通信	368
5-6-7	测试总公司与分公司的 VPN 连接	370
5-7	企业网络集成智能卡身份安全验证与密码管理	372
5-7-1	企业网络身份安全验证的管理	373
5-7-2	RSA SecurID 与智能卡的结合	379
5-7-3	个人密码的最佳管理方案	380
5-7-4	小结	382
5-8	企业无线局域网络最高安全规划指引	382
5-8-1	物理的安全规划	383
5-8-2	技术层面的安全设计	385
5-8-3	服务器端系统架设说明	387
5-8-4	集成 SQL Server 的记录设置	389
5-8-5	客户端连接组件设置说明	391
5-8-6	证书自动注册设置说明	393
5-8-7	小结	394
5-9	WSUS 补丁更新网站的架设与管理	394
5-9-1	WSUS 的新特色	395
5-9-2	WSUS 服务器的硬件需求	396
5-9-3	WSUS 服务器和客户端的软件需求	396
5-9-4	各类部署架构说明	397
5-9-5	网络环境设置说明	403
5-9-6	设置组策略的更新组件	404
5-9-7	建立更新的目标组	406
5-9-8	如何移转旧版 SUS 至新版 WSUS	412
5-9-9	Microsoft Baseline Security Analyzer 2.0	414
5-9-10	小结	415

5-10 数字签名与邮件加密的应用	416
5-10-1 数字签名与邮件加密技术简介	416
5-10-2 设置数字签名与邮件加密运行环境	417
5-10-3 收发带数字签名并加密的邮件	422
5-10-4 小结	429
5-11 Forefront Client Security 介绍与部署指南	429
5-11-1 Forefront 产品简介	429
5-11-2 Forefront Client Security 安全防护技术概述	432
5-11-3 关于部署 Forefront Client Security 的各项软硬件需求说明	434
5-11-4 Forefront Client Security 安装说明	436
5-11-5 Forefront Client Security 常见技术问答	438
5-11-6 小结	442
5-12 实战: ISA Server 集成 Terminal Service 最佳化安全部署	442
5-12-1 搭建网络架构环境	443
5-12-2 程序安装与组件设置	444
5-12-3 TSWEB 安全连接解决方案 (一)	445
5-12-4 TSWEB 安全连接解决方案 (二)	449
5-12-5 关于 Terminal Service 的网络负载平衡规划	451
5-12-6 小结	453

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值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,