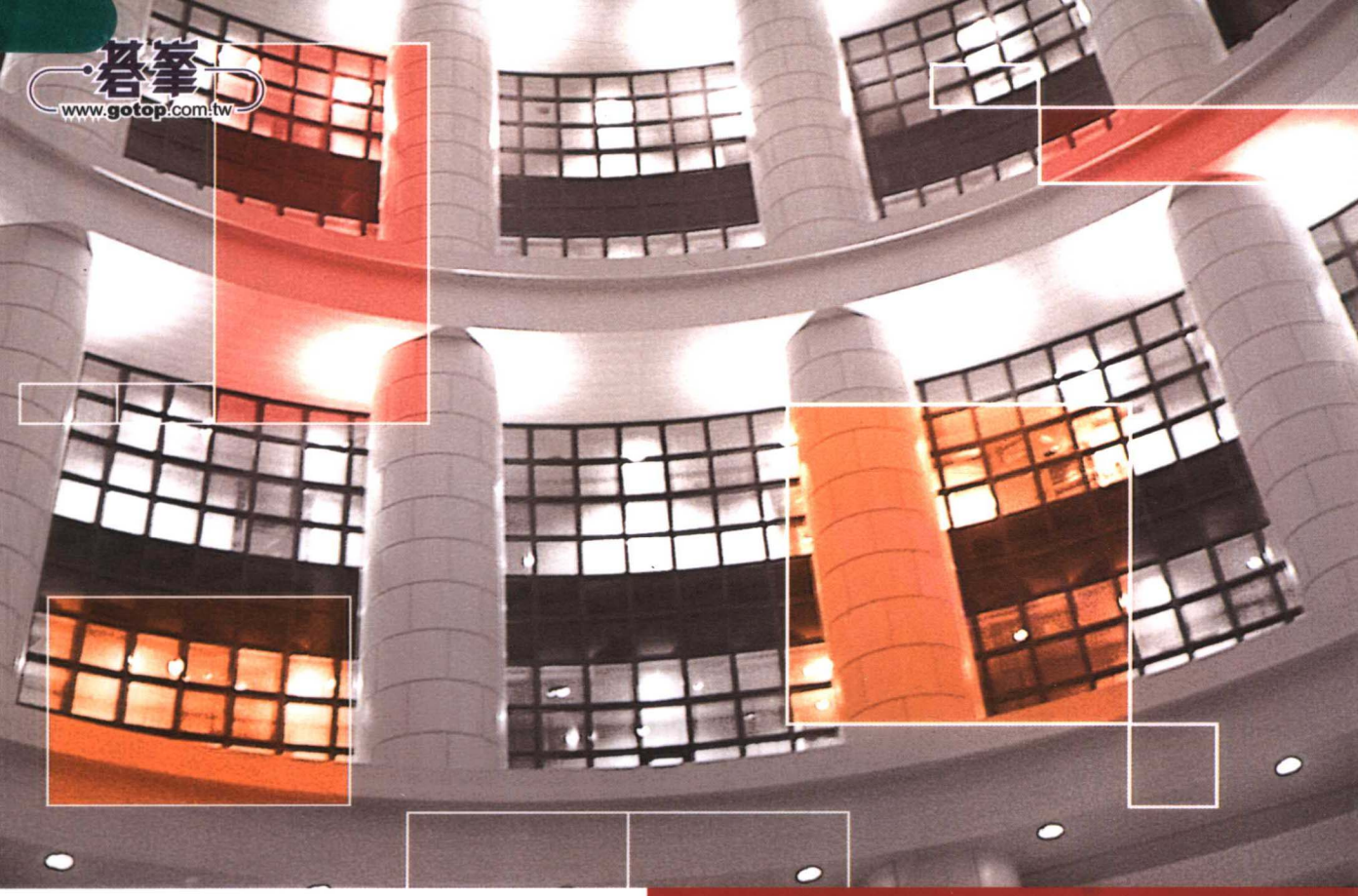


系统安全管理宝典

Microsoft® ISA Server 2004

顾武雄 著

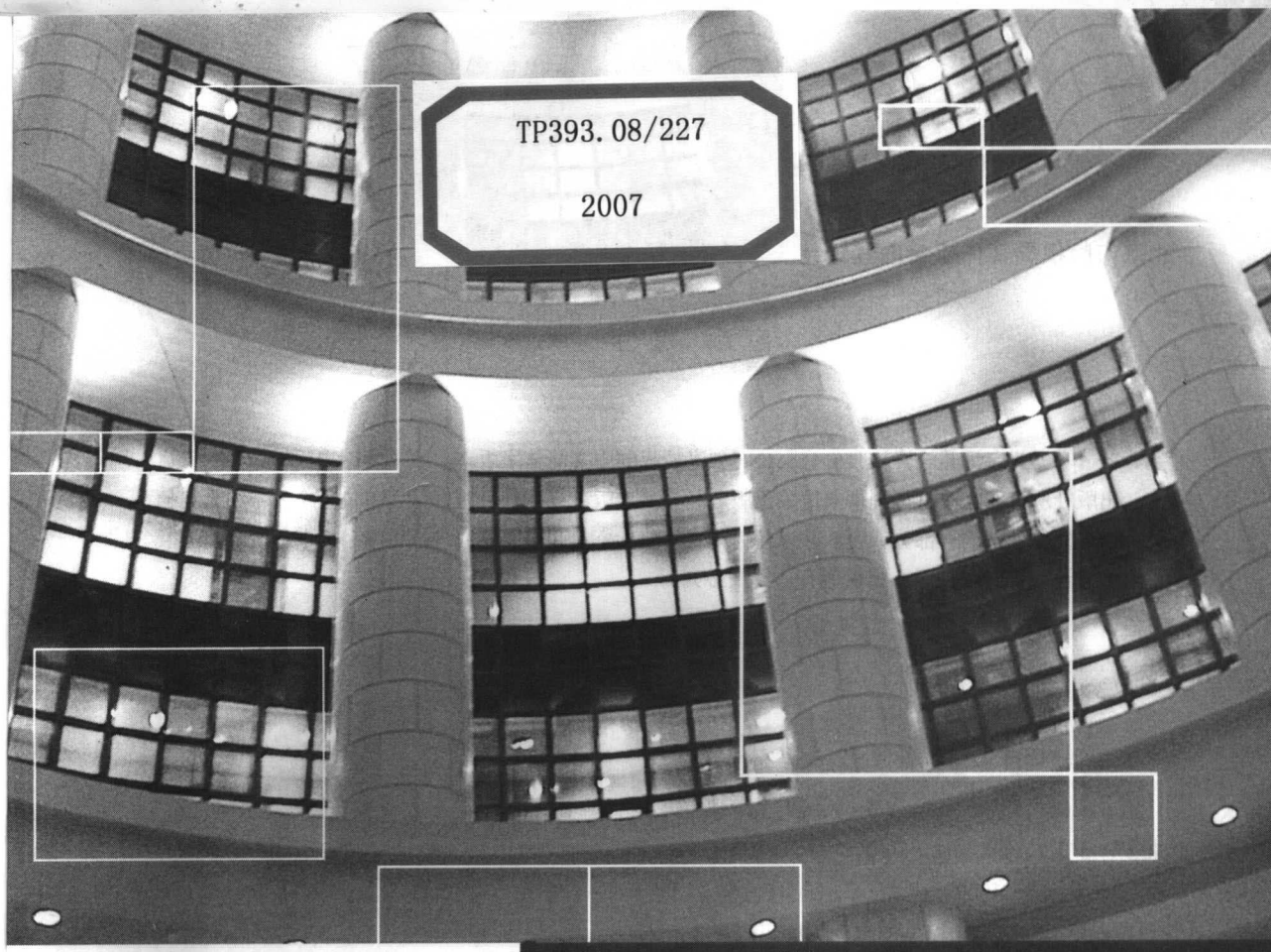
- 信息安全、防火墙及缓存服务的基础导论
- 最新Microsoft ISA Server 2004部署与管理
- 企业整体防病毒网的规范与配置
- Software Update Service企业更新系统的配置
- Right Management Service配置与管理
- SharePoint Portal Server 2003配置和管理
- System Management Server 2003配置和管理
- Microsoft Operations Manager 2005产品技术介绍

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

Microsoft®

ISA Server 2004

[redacted]



系统安全管理宝典

Microsoft® ISA Server 2004

顾武雄 著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

北京市版权局著作权合同登记　图字：01-2005-4563 号

版　权　声　明

图书在版编目（CIP）数据

Microsoft ISA Server 2004 系统安全管理宝典/顾武雄著.
北京：中国铁道出版社，2007.8
ISBN 978-7-113-07610-8

Ⅰ.M... Ⅱ.顾... Ⅲ.计算机网络－防火墙－应用软件，
Microsoft ISA Server 2004　Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2007)第 030107 号

书　　名：Microsoft ISA Server 2004 系统安全管理宝典
作　　者：顾武雄
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
策划编辑：严晓舟　郭毅鹏
责任编辑：郭毅鹏　郑　双
封面制作：白　雪
责任校对：李　旸
印　　刷：北京新魏印刷厂
开　　本：787×1092　1/16　　**印张**：28.5　**字数**：699 千
版　　本：2007 年 8 月第 1 版　　2007 年 8 月第 1 次印刷
印　　数：1～4 000 册
书　　号：ISBN 978-7-113-07610-8/TP・2266
定　　价：42.00 元

序

当前我们处在一个网络科技蓬勃发展的年代，因为网络的广泛应用，人们彼此的信息传送变得没有国界之分，让您在购物时不需要上街，在家里就可以完成银行查账或转账，让企业的整体运行效率在网络之中大幅提升，让懂得应用它的人快速致富，这都是网络科技的先进带来的正面效应。但在它的四周也潜伏着可怕的危机，例如，您的重要信息可能随时被监听，您的企业运行可能随时停止。对一个企业来说在享受网络科技带来的便利的同时，完善的信息安全规划也是不可或缺的，一定程度上它将影响到企业的整体运营和盈利。如何才能构建出安全的企业网络呢？就请细细品味此书的内容吧！

书籍的写作除了需要过人的毅力，更需要的是秉承服务大众的精神和理念。当初写这本书时的构想也仅仅是因为看到ISA Server 2004 Beta 1 管理界面，想到过去自己也曾出版过ISA Server 2000 的书籍，但是内容并不很理想。因此便开始构思这本书的整体架构，期待这本书的内容不仅能提供给读者 ISA Server 的构建和管理，更要以 Microsoft 操作平台为主线，以完善的信息安全规划为目标，写出一本品质优秀的信息安全管理集成应用手册。

ISA Server 2004 的发行提供了全新的直观管理界面，以及更细微的安全控制管理机制，此外更提供了贴心的简体中文版，让初次使用 ISA Server 2004 产品的读者能够快速上手。而在功能部分，除了提供多重网络安全控制管理机制外，更加强了超越传统式防火墙的应用层（Application Layer）过滤功能，并且对于高效的高速缓存服务，提供了比前一个版本更加细微的管理能力。如此完美的呈现，突出了 Microsoft 对信息安全领域的重视，因此 ISA Server 2004 的面世必将在全世界防火墙软件的应用市场上引起一次革命。

顾武雄

2006 年 12 月

前 言

本书以 Microsoft Windows 操作平台为基础，企业信息安全为主线，详细说明了企业网络安全和各类管理系统的构建规则。对每一位有不同学习需求的读者，可以选择阅读不同产品的技术文章；然而对于初学者或是刚进入 IT 以及信息产业的技术人员来说，建议读者最好从第 1 章开始来依次阅读 Microsoft 相关系统的技术，先树立信息安全的正确观念，以 ISA Server 2004 产品为网络安全的基础，接着再按照本企业中不同系统的需要，选择阅读其他不同产品技术的章节内容。

第 1 章　信息安全入门

在一个企业信息化的过程中，最重要的是什么？是“信息安全”。对于一个忽视信息安全规划的企业来说，使用任何系统到头来终究会是一场空。企业信息安全的整体规划，需要从信息安全概念开始。在本章中，将会学习最简单易懂的重要概念，此外针对企业网络安全的基础——Firewall，将剖析关于软件防火墙之间的差异，以及对 Microsoft ISA Server 2004 的整体技术概述。

第 2 章　ISA Server 2004 系统构建

通过本章指导，读者将可以根据现行企业的网络环境，开始部署 ISA Server 2004 的服务器端和客户端，在完成初步的系统构建之后，必须先完成客户端对网络的访问规则设置，以及实时监控服务器端的运行状态。

第 3 章　Internet 服务器防御

对企业内部一些对外公开的网络服务器，如 Web、FTP、Mail 和 DNS 服务器等，必须做好适当防护措施，才能避免企业网络受攻击和入侵的威胁。在本章内容中，读者将学到各类网络服务器的防范技巧。此外，也会了解到黑客一贯的攻击和入侵模式，让读者真正做到知己知彼，百战百胜。

第 4 章　ISA Server 2004 高级配置

对需要更安全的数据传输的企业来说，为了避免数据在传输过程中遭到窃取，需要结合更安全的数据传输通道 VPN 和 SSL 技术，此外，针对企业内部 Internet 服务器的构建，建议在专用 Internet 服务器的网络区段 DMZ 配置，最后还需要读者懂得使用报表和警告功能，作为强化防火墙安全配置的参考依据。

第 5 章　加强企业信息安全防范

只靠防火墙的构建就能让企业的网络安全万无一失了吗？对于任何规模的企业信息环境来说，防火墙的构建只是网络安全的第一步，还需要有一套完善的企业防病毒网络和垃圾邮件过滤系统的规划以及即时的安全增强措施，这样，面对外来的恶意侵害才能进行有效地遏止。对于重要商业机密文件外流的安全漏洞问题，请阅读本章最后的 RMS 使用说明来解决。

第 6 章　软件开发工具应用（SDK）

是否想过自己编写小程序来管理 ISA Server 2004 呢？本章会介绍 ISA Server 2004 相关的

SDK 应用说明，供想自定义一套管理方案的用户参考。

第 7 章　SharePoint Portal Server 2003 配置和管理

如今，企业网站的有效管理已成为一项炙手可热的话题。在本章内容中，读者将学到最快速规划和构建一个企业入门网站的方法，使企业中长期以来难以有效改善的网站管理问题得以解决。

第 8 章　System Management Server 2003 配置和管理

对于一位 IT 人员，信息管理和软件的部署问题是复杂的工作。本章内容将协助读者学习在 Microsoft 产品里唯一可以解决上述问题的系统管理产品 System Management Server 2003，读者阅读完本章之后，将会因为它的强大功能而感到高兴。

第 9 章　Microsoft Operations Manage 2005 产品技术介绍

面对机房中眼花缭乱的服务器端应用系统如何管理以及全面掌握的问题，读者可以通过全新设计的 Microsoft Operations Manage 2005 产品，轻松地快速部署集中化管理的集成环境，让 IT 人员真正提高效率。

附录

在本书附录中，作者额外编写了 Microsoft Exchange Server 2003、Live Communication Server 2003 和 Project Server 2003 的配置说明，提供给初学者和有额外系统集成需求的管理者参考，此外还附加了 ISA Server 2004 支持工具和性能对象的使用说明，并且提供了一篇升级的使用说明，以方便有升级需要的读者参考。

编　者

2007 年 1 月

目 录

第1章 信息安全入门

1-1 信息安全的重要性

网络科技的迅速发展激发了企业对于信息安全的重视，网络不仅提高了企业间的业务效率，加速了彼此间的数据传输速度，同时也使人与人之间和公司与公司之间的重要信息安全传递面临着极大的挑战。

信息安全究竟有多么重要？根据美国 CSI/FBI 2004 年的《计算机犯罪与安全调查报告》中的数据显示，2003 年仅遭受计算机病毒破坏而造成损失的案例就有 254 起，至于损失的总金额更是高达 27 382 340 美元，事实上这还不是最糟糕的情况。由于网络安全配置上的疏忽，而遭受 DoS（Denial of Service）攻击所造成损失的案例有 111 件，虽然发生的总件数远低于病毒，但损失的总金额却高达 65 643 300 美元。如果我们把这两部分所造成的损失加起来，数字是非常巨大的。由此可见，在享用信息科技所带来便利的同时，对信息安全的重视更是一点不能马虎，一旦忽视了它，可能下一个因遭受破坏而损失惨重的就是自己了。

对企业信息安全的整体规划，可从以下两个层面来着手。

- 技术层：这部分主要是依靠 IT 人员的专业技能将现今市场上有效的网络安全产品集成到企业内部。例如防火墙、防病毒系统、入侵检测系统（IDS 或 IDP）、加密验证系统等。
- 管理层：这部分重点是对人的管理，使用有效的信息安全策略来管理企业内部信息安全。根据统计，因为不正当的内部网络访问和未经授权验证而访问所造成损害的比例分别为 80%和 71%。

完成上述规划后，还要保证企业网络信息环境达到机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）3 大需求。

配置防火墙的目的

- 过滤进出企业的网络数据包：对于进出网络的数据包传输，都必须使用不同的通信协议和通信端口进行通信。因此，通过防火墙的网关管理，就可以只让有必要的通信端口打开，维持企业网络的基本安全。
- 记录进出企业网络的连接：防火墙的工作内容，除了要能够进行网关的安全管理之外，还必须要记录每一个进出的连接，以便管理员以后进行安全连接访问分析，可以将危害内部网络安全的连接阻止。
- 避免主机直接暴露在 Internet 上：通过防火墙的配置可以将内部的虚拟网段与 Internet 上连接的其他计算机进行最重要同时也是最基本的隔离，如此一来，即使终端遭受攻击，也不会马上受到破坏。然而这仅仅是第一层的防护而已，除此之外还

必须要依赖防火墙本身的具体防护机制来进行多层防护。

- 防范日益猖獗的网络病毒：当今病毒与十几年前的病毒类型相比，已经大不相同，更确切地说是“技术规格”的巨大差异！这也是由于网络科技发展迅速所致。以往病毒依靠磁盘的访问进行感染，病毒传播速度很慢，因此进行危机处理时的缓冲时间也相对较长。如今大多数病毒都是通过网络系统漏洞或打开的通信端口进行迅速传播，因此在目前的企业信息网络环境中，防火墙早已成为最基本的配置，在此提醒读者随时检查自家的“门窗”是否安全。

防火墙无法防范的源

- 最新的黑客攻击手法：黑客的攻击行为与所用的工具软件日新月异，五年前的防火墙在防护功能上的设计较为简单，因此如果用于与当今各种新类型病毒抗衡会显得力不从心，因为编写病毒程序的人不仅要找出各类系统的漏洞，更要无声无息地通过防火墙的阻碍。
- 内部人为破坏：所谓家贼难防，在这里是指网络管理员。虽然可以通过许多精密仪器来监测外来攻击或窃取，但却时常忽略内部本身的管理问题，因此不要什么事都去依赖科技手段。
- 多条线路：如今许多企业内部可能都有两条以上网络线路，根据调查，除了因为线路租金低廉外，主要都是为了根据不同的用途来管理带宽流量与访问安全问题。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，还可以通过外部拨号连接的方式进行数据传输或远程控制。因此，如果网络病毒或黑客入侵不从正面攻击，防火墙也就无能为力了。

防病毒系统无法防范的源

- 最新感染的新病毒：由于当今网络的普及，导致病毒传播的方式已由过去的磁盘感染转换为通过网络的感染，因此从新病毒的产生到传播至整个国家乃至全世界，传播速度可谓是迅雷不及掩耳，让无辜的用户避无可避。尽管全世界有许多家防病毒厂商在发现病毒的第一时间内都会发布有关该病毒可能危害的新闻稿、更新网页和发出电子邮件等，让用户能够尽快上网进行病毒码更新或系统安全更新，为何还会有大量的受害者呢？原因很简单，因为多数的用户都没有阅读这些信息的习惯并且警觉性不够高，或即使知道了也不认为下一个中毒的会是他；其次则是病毒的传播速度太快，而防病毒厂商的动作较慢，就像电影中的情节一样，往往在罪犯实施了犯罪之后，警察才会到现场来，类似这样的剧情应用到现今的信息市场中，可以说是再贴切不过了。
- 管理员的疏忽：一家公司的信息环境，无论规模大小，信息都全部掌握在IT人员手中，而不是老板。这么说可能会遭到许多IT人员的反驳，原因是如果老板不投入资金是什么事也做不成的，不过反过来想想，是不是这也说明管理员的提案中有些遗漏或不足以说服老板的理由呢？如何避免这样的窘境呢？建议用户可以找一家优秀的并且最具口碑的系统集成商来协助自己。一旦有了详细的采购预算却仍然不好的

情况，就要归罪于规划的落实和合作厂商的专业能力了，因为防病毒的规划必须做到疏而不漏的地步，该花费的地方一毛钱也不能省，不该花费的地方一分钱也不能浪费，因此在采购之前请详细列出兼顾内外具体防范机制，对于每一个可能的死角都不要忽视，因为它随时可能成为连夜加班和造成巨大损失的致命伤。

- 系统本身的安全漏洞：如今的网络病毒泛滥成灾，绝大部分是通过操作系统或网站应用程序的漏洞（如红色代码 Code Red）深入到企业内部网络之中，因此，这种类型的病毒，也可以说是一个专门查找漏洞的破坏程序，绝不是单靠防病毒系统的部署就可以进行有效防御的，因此从客户端到服务器端的每一台计算机都必须保持在最新系统更新状态，这部分的规划与实施可以参考本书关于 SUS 或 SMS 的章节，此外防火墙的规划配置也是重要的防御方法。
- 远程访问的危害：根据笔者调查，如今大多数公司都完成了防火墙与防病毒系统的配置，在此我们假设这些企业对于内部网络的防病毒与系统更新措施都已做的尽善尽美，可是对于部分启用远程访问功能（如 RAS 或 VPN）的企业来说，它们针对通过远程访问身份验证的合法用户是如何进行安全防范的呢？答案是：几乎想都没想过这个问题。如此一来这个信息安全死角随时可能一触即发，从而使企业网络的信息安全建设倒塌。为什么会有这么严重后果呢？事实上原因很简单，举例来说，一旦用户回到家里或到外地出差时，因为公务的需求需要通过 VPN 连接到企业内部网络进行访问，此时如果用户计算机所感染的病毒比企业中的防病毒系统病毒码更新，再加上该用户是以网络管理员的身份登录，那么后果可想而知。除了病毒的远程感染是一大威胁之外，远程客户端的系统更新状态也是一大主因，对于这些可能无法控制的远程客户端而言，管理员需要有更好的防护机制来解决这类问题。在此读者同样可以参考本书有关 VPN 隔离控制（Quarantine Control）的章节。

1-2 构建安全的电子化环境

本节将与各位读者一同探讨如何构建安全的电子化环境。

首先，我们必须对信息安全的构建有一个基本认识，它是影响企业信息安全因素的根源，它不仅需要完善的软硬件产品防护，更重要的是制定有效的企业信息安全策略以进一步管理人的因素，图 1-1 是笔者自己定义的“影响企业信息安全的六大因素”。

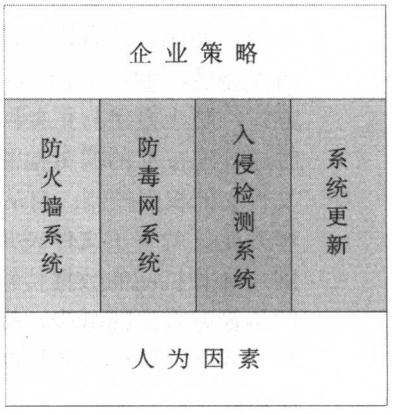


图 1-1 影响企业信息安全的六大因素

根据计算机安全协会从过去到现在的调查，企业发生信息安全危害时，直接原因绝大部分都是人为因素，然而人为因素直接关系的是企业信息安全策略的落实，其中最重要的就是员工的培训与安全意识的提高。

至于如何防范人为因素可能造成的信息安全危害，根据笔者的自身经验可将其归纳为以下几个重点。

- 员工账户密码的管理：对每一位有企业内部访问权限的员工账户和密码，都应制定要求用户

定期更新的策略，以及密码长度（如不能少于 8 个字符）与复杂性的定义（如密码不可以与账户名称相同），如此一来才能有效防止账户密码被不法分子破解。例如，图 1-2 所示的就是 Windows 密码策略设置。

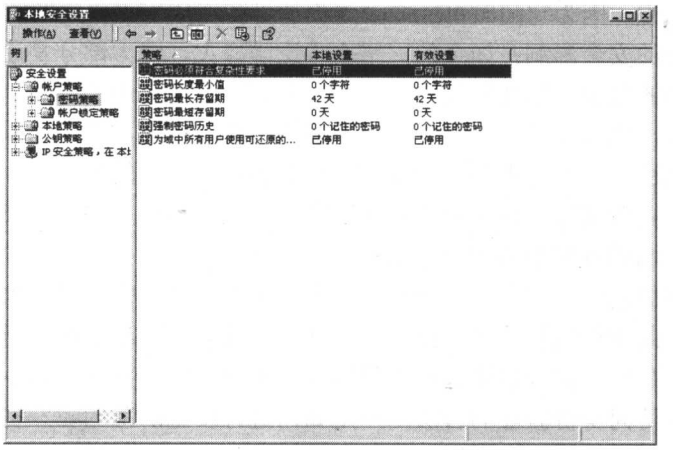


图 1-2　Windows 密码策略设置

- 对外部连接访问的控制：关于员工对 Internet 的访问，一般情况下企业都不会刻意的加以限制，但是对于有危害性的网站还是有必要限制访问的，还要禁止个人下载的软件在本地计算机安装执行，例如许多员工可能会通过 QQ 与 MSN 这类的即时通信软件与外部其他用户互相传输文件，这些都有必要考虑加以限制。
- 本地计算机访问的控制：目前很多企业都要求员工所使用的个人计算机没有光驱、软驱并且禁用 USB 接口，所有本地计算机需要安装的软件都是直接通过内部文件服务器来提供的，这样的措施除了可以防范机密外泄，最重要的是可以大幅降低病毒的感染与传播。
- 外部计算机的访问限制与过滤：企业间有许多平常往来频繁的供货商或客户，这些人可能时常因为业务或技术支持上的需要，会将自己的笔记本电脑直接在企业网内部连接。如果该计算机本身带有病毒，它所造成的危害恐怕不是一两天内可以消除的。像这样的问题笔者身边的客户就曾发生过好几回，因此目前有许多的企业对于外来计算机的内部连接，通常会采用以交换机来分割 VLAN 的方式，防止直接与重要网段或服务主机连接，同时进行连接前的病毒检测加以防范。
- 文件夹的权限控制：自从有 Windows 网络操作环境开始，就有了文件夹共享概念，它方便了局域网内计算机间的数据传输，让过去普遍使用磁盘的传输方式大幅减少，提升了平时工作的效率。对于共享文件夹，权限的设置也很重要，如图 1-3 所示。

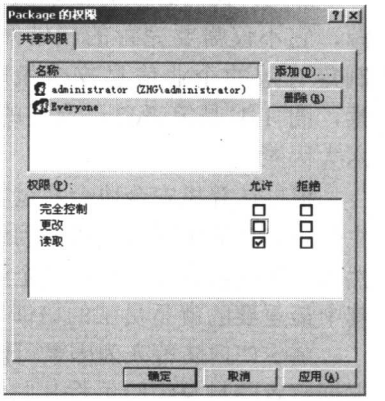


图 1-3　文件夹的共享权限设置

虽然文件夹的共享设置方便了许多用户平时工作中的文件传输，但它同时也成了企业网络安

全的致命伤。因为在 Windows XP 以前的操作系统，当用户共享了文件夹之后，经常忽略了对文件夹共享权限的设置，这使得一些别有用心的人或网络病毒（如红色代码）利用此安全漏洞进行大规模破坏，原因是在默认的共享状态下，文件夹的共享权限是所有人（Everyone）都可以来进行“完全控制”的，而黑客或病毒当然也属于 Everyone 的成员之一。所以在安装 Windows XP 操作系统之后，当将文件夹进行共享之后，默认所有用户的权限设置为“读取”。

无论是对文件夹的共享权限，或者是对 NTFS 的文件夹进行权限设置，一旦这些文件被别有用心的人外泄后，原先设置的文件权限也将随之消失，因为这些文件的权限设置都是依靠现有操作系统本身实现的。

- 内外连接登录的审核：目前 Windows 2003 Server 的登录审核功能默认是启用的，但是在先前的版本默认都是未启用的。除了操作系统本身的审核功能需要启用外，其他数据库的访问审核也都应当启用这项功能，例如 SQL Server 本身所提供的 Profile 工具就可以用来跟踪用户的访问行为，并且将这些记录直接存储在指定的数据表中，如此一来就能够随时知道哪些用户在什么时间做了哪些事情，并防范尝试入侵的用户，如图 1-4 所示。
- 重要文件的验证或加密处理：企业内部重要机密文件外泄事故层出不穷，如何进行有效地防范呢？最常见的便是将这些文件加密，使得只有拥有密码的人才能够打开这些文件。

如图 1-5 所示，可以对本地 NTFS 文件系统下的特定文件夹或文件来设置加密属性，如此一来即使文件被其他人盗取也无法打开，像这样的加密属性除了可以应用在个人单机操作环境之外，也可以结合 Active Directory 与 CA 证书服务，使局域网的共享文件夹也可以有加密的设置，只有特定用户可以访问它。关于这部分的综合应用，在后面的章节内会有进一步说明。

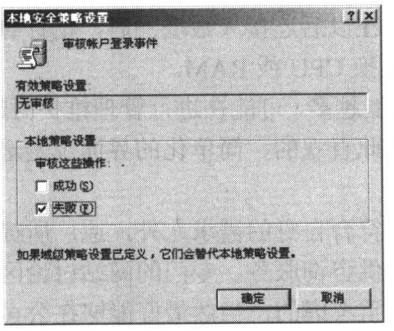


图 1-4　审核 Windows 登录事件

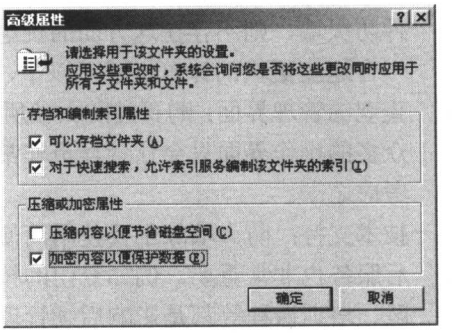


图 1-5　针对文件或文件夹启用加密属性

并非所有的文件内容都是完全不让特定员工知道的，许多重要文件内容也需要对内公开，但又不能使该内容外泄，此时对这些文件的安全控制就不能通过使用锁定密码或加密属性来处理，而是需要以用户针对内容访问权限的验证机制来处理，这样的权限验证机制将可以有效地限制用户对该文件内容的转发、打印、画面截取、复制、另存为等行为。关于此验证方法，在第 5-6 小节的 RMS（Rights Management Service）应用部分中，将会有具体的使用说明。

除了笔者上述整理的针对人为因素的基本安全防范机制外，也可以参考目前国际上关注的 BS7799 信息安全系统，它是一套完整的信息安全计划，来自于英国标准协会（British Standards Institute，BSI），目前已被 ISO 认可为国际标准，它主要为企业提供有关信息安全

方面的帮助，包含了获取有效的信息安全管理指南、安全责任归属、风险评估、人为信息安全防范、病毒防范等。该系统对于企业信息安全的管理层有很高的加分效应，关于它的详细介绍，可以参考相关网站或参加 BS7799 完整课程的培训。

软硬件防火墙的优异性

在了解了有关信息安全对于企业电子化的重要性之后，接下来我们需要开始评估市场上众多软硬件防火墙之中，哪一类型的防火墙系统适用于企业。在开始介绍软硬件防火墙间的差异性之前，让我们先来对防火墙的采购须知有一些了解。

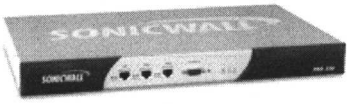
- 质量认证：采购的防火墙要通过国际计算机安全协会（ICSA）和通信安全机构（CSE）认证。
- 权限控制：对于用户的对外连接访问，提供针对客户端计算机或附加的用户访问控制列表，用于基本的网络流量分配管理。
- 审核功能：对于未经验证的连接访问，提供审核日志文件供管理员检查，方便于以后的跟踪与进一步的访问控制。
- 报表功能：每一天、每一周、每一个月都应有详细的评估报告，如今许多软硬件防火墙都提供该功能，少部分需要额外购买。报告的查阅可使管理员得知内部对外的连接状况，例如，哪一种通信服务所占用的带宽最大，哪一个用户或计算机的连接占用的带宽最多等。此外对于外部计算机对内部 Internet 主机的访问状况和安全问题都可以在报表的检查中得知。
- 连接人数的限制：通常防火墙使用的年限至少在 3～5 年，甚至于更久，因此，必须注意它的连接负载限制是否可以符合企业在未来连接人数上的增加需求。如果是软件防火墙，则不存在这方面的疑虑，只需要在以后连接人数增加时，把计算机换成一台速度更快的计算机就可以了，或者只更换 CPU 或 RAM。
- 直观的管理界面：购买的防火墙所提供的功能越多，可能在进行管理维护时越麻烦，众多的操作界面只会让管理员非常痛苦，因此直观的、简单化的界面也是选购时的考虑之一。
- 技术支持：防火墙除了要使用简便以及功能符合自身的需求之外，原厂所提供的售后服务也非常重要，例如专门的技术窗口提供咨询服务、专门的网站讨论区与资源区、培训课程等都是影响后续管理而需要着重考虑的，当然最好能够在公司附近有技术支持经销商，这样在需要获得帮助时可以就近得到服务。

上述几点只是针对防火墙在采购时的基本考虑，事实上，用户可能还需要其他特殊的功能，如 VPN、HA、带宽管理、集成防病毒系统、集成入侵检测等，关于这些需求都可以在目前的信息市场上得到满足。接下来就让我们一同看看各种软硬件防火墙。

硬件防火墙

图 1-6 所示的 4 款硬件防火墙是相当知名的防火墙品牌，无论是在中小企业、大型企业，还是在政府机关、学校单位都能够经常见到，其中以 CISCO PIX 系列的产品在国际最为知名，尤其在大型企业与政府机关使用最为广泛。相信许多公司在配置防火墙时，IT 人员都会仔细

地比较每一种品牌的价格与规格，并且也可能在选择软硬件防火墙间犹豫。那么究竟哪些是在采购时必须评估的内容呢？在表 1-1 中列举了软硬件防火墙的比较内容。



参考网址：http://www.sonicwall.com

参考网址：http://www.netscreen.com

参考网址：http://www.cisco.com

参考网址：http://www.watchguard.com

图 1-6　4 款知名的硬件防火墙

表 1-1　软硬件防火墙比较

比 较 内 容	软件防火墙	硬件防火墙
扩展性	高	有限
简易性	较复杂	较简易
可靠性	高	视规格而定
效率	视硬件平台而定	高
集成能力	高	低
价格	低	高

整体看来，软件防火墙所提供的各项性能都比硬件防火墙优越，但是软件防火墙系统由于是配置在现有的操作系统上，如 Linux 或 Windows，因此操作系统漏洞常常会成为黑客的攻击与入侵的目标，所以对于管理员来说就需要投入更多的时间和精力来配置它。

除了表 1-1 中列举的考虑因素外，根据笔者的经验，有许多企业希望能够集成 Active Directory 用户的验证功能，这直接体现了 ISA Server 的功能优势。至于硬件防火墙，如果需要集成 AD 用户的验证功能，则必须在规格上支持 RADIUS Server 才能够搭配 Windows Server 2003 所提供的 RADIUS 验证服务。

在本节最后，让我们比较一下 ISA Server 与 Windows XP/2003 Server 中的 ICF（Internet Connection Firewall)服务之间的主要差异(见表 1-2)，以便使管理员在选择 Microsoft Windows 防火墙时有个依据。

表 1-2　ISA Server 与 ICF 的比较

功 能 特 性	ISA Server	ICF
操作平台	需额外购买，可安装在 Windows 2000 Server、Windows 2000 Advance Server、Windows 2003 Server 标准版以及企业版	内置在 Windows XP / Windows Server 2003 所有版本中

续上表

功能特性	ISA Server	ICF
适用对象	适合各种规模的企业网络环境使用，可搭建在复杂的多重防火墙需求环境	适用于小型企业以及个人用户
安全认证	荣获 ICSA 安全认证	无
功能	● 支持数据包、状态、应用层连接过滤 ● 支持多重网络安全控制 ● 支持大量的网络应用程序 ● 集成企业虚拟专用网络（VPN） ● 强化系统安全 ● 支持入侵检测功能 ● 智能型应用程序过滤 ● 支持 Windows AD、Radius、RSA 身份验证技术 ● 企业因特网服务器发布 ● 集成 Exchange Server 高级安全防护 ● 报表分析功能 ● 连接记录实时监视功能	● 状态数据包过滤 ● 静态通信端口对应设置 ● 不支持应用层过滤技术 ● 除了检查源连接的 IP 地址之外，无数据包内容检查能力
部署环境	● 边界网络（DMZ）的体系结构部署 ● 控制用户的对外连接访问 ● VPN Server 集成配置 ● SSL 的安全通信环境部署 ● 正向、反向、分布式、层次型缓存部署	针对单一计算机的安全防护，或者少数客户端计算机环境中的共享连接防护
访问控制	通过防火墙的访问规则定义，有效管理客户端计算机、用户、组的对外访问，并且可定义访问的目的地、分配、HTTP 内容	有限的对外连接访问控制
企业 Internet 服务器的发布	支持安全地发布企业 Internet 各类服务器服务，以避免直接暴露于外部 Internet 中	无企业 Internet 服务器发布功能
日志文件格式	● W3C 文件格式 ● ISA Server 文本文件格式 ● 支持 MSDE、SQL Server	W3C 文件格式
扩展性	可与许多合作厂商所发行的 ISA Server 过虑器集成，例如网关防病毒系统、文件下载筛选器、高级报表分析器、高级连接控制等，此外还可使用 ISA Server 所提供的相关 SDK 开发套件来自行开发，以扩展或加强 ISA Server 现有功能	无扩展性
缓存与 Proxy 功能	支持企业级的缓存服务功能	不支持缓存服务

ISA Server 2004 新特性概述

从早期的在 Windows NT 平台下的 Proxy 2.0，到 Windows 2000 Server 平台下的 ISA Server 2000，再到如今支持体系结构的在 Windows 2003 Server 环境下的最新 ISA Server 2004，每一次的全面改版，都让人耳目一新，原因在于无论在功能还是操作界面上，每一次改版都远远超越了先前的版本。想必这是因为它在整个企业网络安全体系结构中扮演着居于第一线对抗外敌、保卫家园的角色，因此对于每一次的全新设计，都必须符合现今信息安全的潮流，以