Microsoft ISA Server

建置与管理

顾武雄 编著

Internet 黑客的入侵与攻击行为让您感到不知所措吗？

您总是觉得公司连接Internet网站的速度不够快吗？

当公司对外只有一组ADSL所提供的IP地址时，如何让公司内部所有用户端主机，皆可安全又快速地连接Internet呢？

以上的烦恼将通过本书彻底帮您解决！

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

Microsoft ISA Server 建置与管理

顾武雄 著

中国铁道出版社
2001年·北京

（京）新登字 063 号

北京市版权局著作权合同登记号：01-2001-4265 号

图书在版编目（CIP）数据

Microsoft ISA Server 建置与管理/顾武雄著 －北京：中国铁道出版社，2001.12
ISBN 7－113－04410－7
Ⅰ.M… Ⅱ.顾… Ⅲ.计算机网络-防火墙-应用软件，Microsoft ISA Server Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 075030 号

书　　名：Microsoft ISA Server 建置与管理
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：苏　茜
特邀编辑：邓庆容
封面设计：孙天昭
印　　刷：北京市兴顺印刷厂
开　　本：787×1092　1/16　印张：13.5　字数：323 千
版　　本：2001 年 12 月第 1 版　2001 年 12 月第 1 次印刷
印　　数：1～5000 册
书　　号：ISBN 7-113-04410-7/TP・631
定　　价：22.00 元

出版说明

由于因特网的快速发展，目前各行各业都陆续地投入到 Internet 市场，例如目前的 B2B、B2C 在全世界的各中小企业应用上皆是不胜枚举。但您知道吗？除了因特网在企业上的应用之外，对于企业内部重要信息的安全性隐藏了多大的危机！当您在因特网上发布企业信息的同时，也是您企业网络面对攻击危机的开始。这其中的受害程度，小则企业网络主机瘫痪，大则损失数千万！这些可能的危机都是不可轻视的，因此才会有所谓的 Firewall、Proxy 等技术出现。目前国内外许多科技公司都有这方面的相关产品，如何选择最简易、最好、最经济实惠的产品，将是大家最关心的话题。

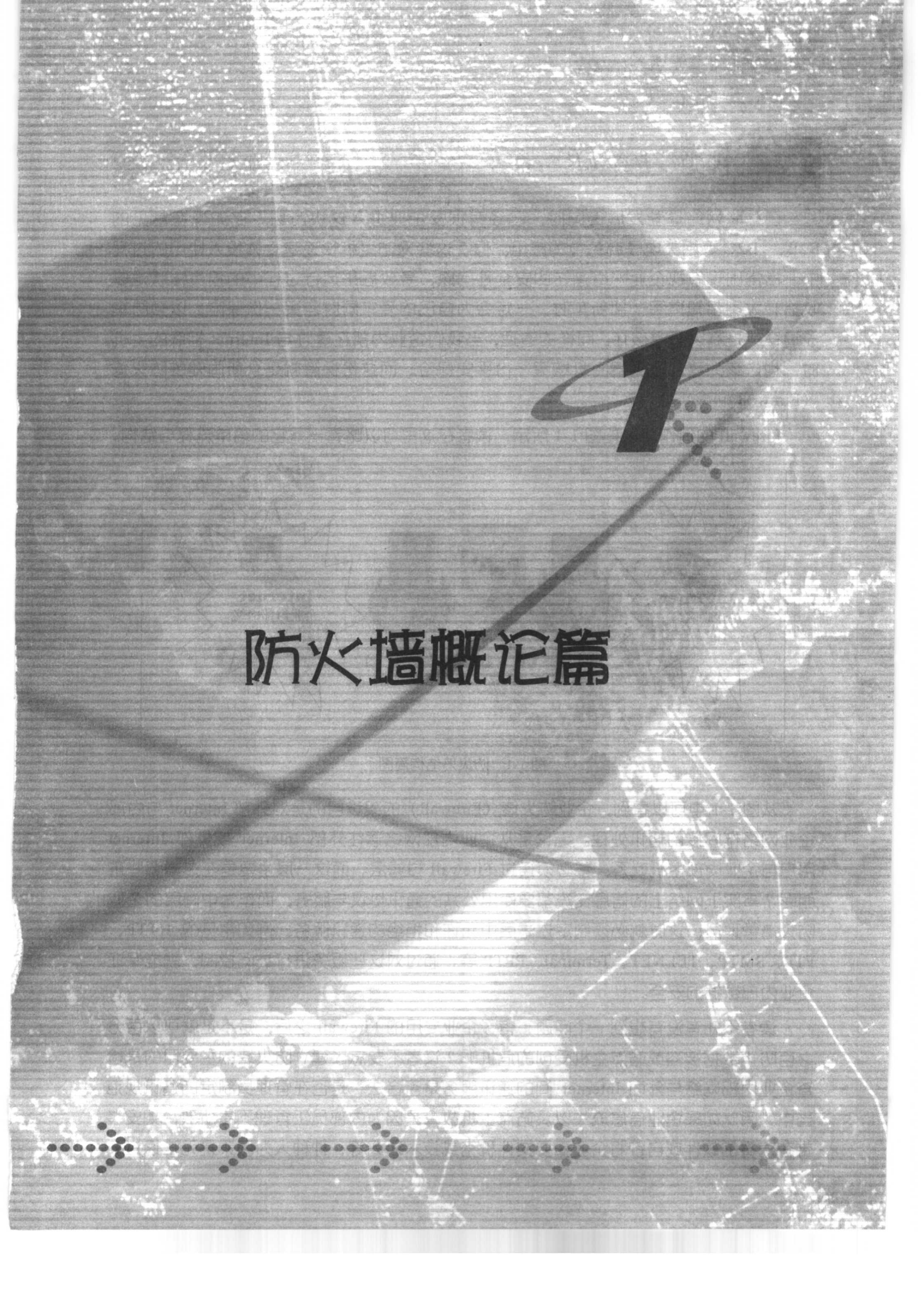
本书将为您介绍 Microsoft .Net Enterprise Server 中的一项产品，关系到整个中小企业网络安全与否的完整解决方案，也就是本书的主题 ——ISA Server 2000 （Internet Security and Acceleration Server）。书中的内容将以由浅入深的方式带领读者进入 ISA SERVER 2000 技术领域的世界，无论您是完全不懂的初学者，或是已经拥有架构 Proxy 能力的工程师，这本技术实务手册将更加提高您个人在此领域上的能力。

Internet Security and Acceleration (ISA) Server 2000 改善了前一版在 Windows NT4.0 平台上的 MS Proxy2.0 许多安全性及缓存上的缺点，提供了更快速、更安全且易于管理的直观性操作界面，并整合了企业级的防火墙系统与高性能的缓存机制。ISA Server 2000 建构在 Microsoft Windows 2000 Server/Advanced Server 操作平台上的安全特性与目录服务功能，无论在巩固系统安全或是加速因特网访问上都有优异的表现。

本书由台湾旗标出版股份有限公司提供版权，中国铁道出版社计算机图书项目中心审选。张瀚文、杨健、葛兰、彭涛、肖志军、廖康良、裘伟力、陈贤淑等同志完成了本书的整稿及排版工作。

中国铁道出版社
2001 年 11 月

目 录



1

防火墙概论篇

1-1 何谓 Firewall Server

在互联网络蓬勃发展的同时，已经有很多企业进入这块市场。比如现在常见的B2B、 B2C 等相关电子商务上的应用。但在这些网站主机快速建立并投入使用的过程中，常常出现忽视企业网络潜在的安全性问题，导致后来运行过程中的损失惨状难以收拾！大家都知道买一部新车时，一定会为自己的爱车同时购买一份保险，以预防车子遭窃或是遭人恶意破坏。同样的道理，当我们企业内部在建立与 Internet 相联的主机时，也应该为这部服务器主机购买一份平安保险；而这份保险就是众所周知的防火墙（Firewall）。

Firewall 的运作可以如图 1-1 所示，读者在这里可以略看一下它的简单流程与结构：

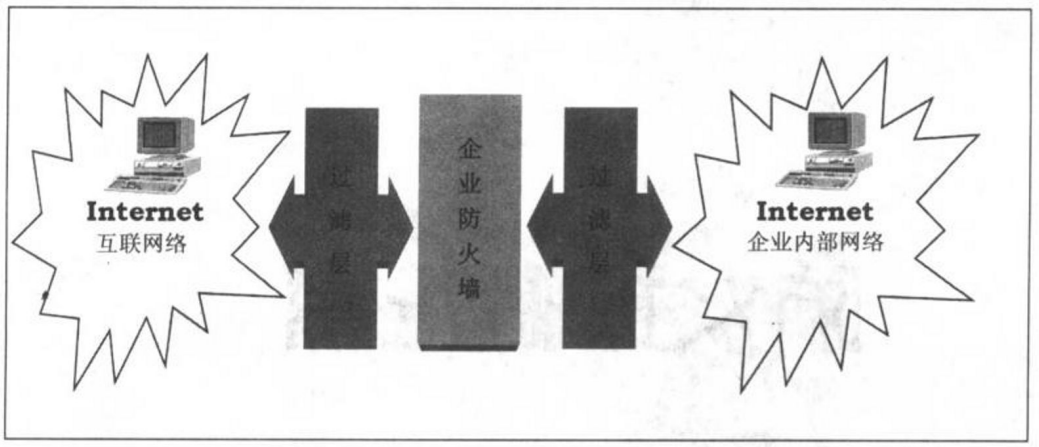


图 1-1 防火墙结构简图

从图 1-1 中可以看到，企业防火墙（Firewall）的架设目的是对外部 Internet 与内部企业网络作间接的通讯处理。无论是从企业内部网络通往外部 Internet 或外部 Internet 用户与企业内部主机联系，都必须通过 Firewall 过滤层。而这一层主要是在过滤哪些东西呢？事实上网络上的信息交流都要使用公共的通讯协议与服务，而作为中间层的企业防火墙管理员，这时就必须制定过滤层中允许和拒绝的通讯服务。例如常见的 HTTP、FTP、SMTP、TELNET、Terminal、PPTP 等。通过对这些服务进行访问控制，就能保证企业内部数据的安全。

读者不知有没有想到一个问题：有了企业专用的 Firewall 之后，是不是就可以百分之百防止数据被盗或站点主机受创的危机呢？读者不要忘了建立防火墙的主要目的是检查企业内部网络与外面 Internet 间的通讯服务是否合法；是否在管理员制定的通讯规范当中。因此如果企业信息流失以及站点主机故障是因为内部员工管理不善所致，如安装带有病毒的软件或自行将企业重要文件机密或技术泄漏等；种种人为因素是无法通过一

部 Firewall 主机就能避免的。所谓“家贼难防”其原因就在这里。

另外，网络间病毒程序的传播途径，常常是通过 Internet Mail 的使用或 FTP 文件传送，导致企业网络主机的故障。所以在建立 Firewall 的同时，管理员也必须为诸如 Mail Server、Web Server、FTP Server 等重要的网络服务器建立一套获得国际间企业认可的防毒软件。总而言之，企业防火墙的建立，必须搭配一套防范由人为因素造成的危机的管理措施。这样才是一套完美的企业网络安全管理建立方案。

1-2 何谓 Cache Server

本小节将介绍 ISA Server 200 的另一项强大功能，即 Cache Server。Cache Server 的结构如图 1-2 所示。

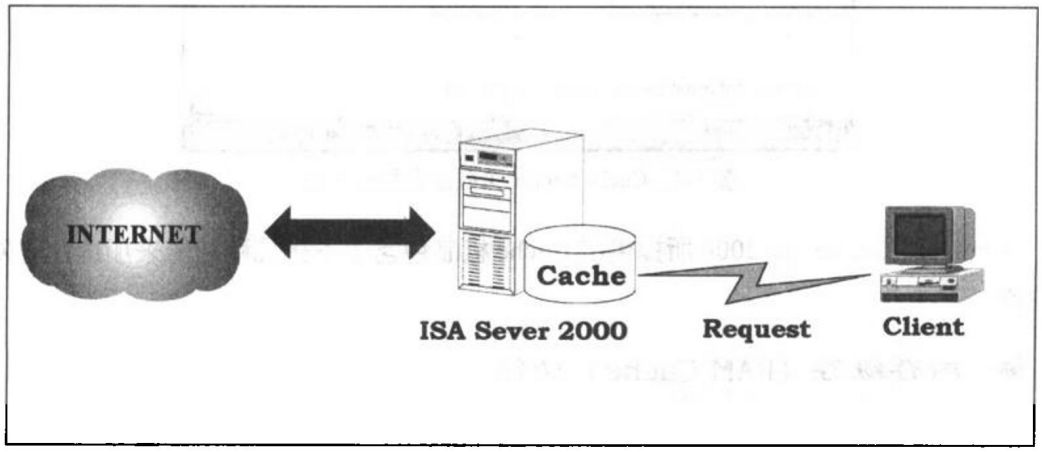


图 1-2　Cache Server 结构简图

从图 1-2 中可以看出，当企业内部的客户端计算机通过 Cache Server 来对外通讯时，Cache Server 会首先检查主机上是否有现存最新的数据来提供给企业内部客户端。如果有的话，则直接由（本机）Local 端来响应用户请求；如果没有的话，则 Cache Server 会从远端取回数据，并将此次取得的数据记录在缓存（Cache）中，以备用户下一次请求使用。当 Cache Server 找不到客户端所要求的网站时，会将错误信息返回给客户端，如图 1-3 所示。

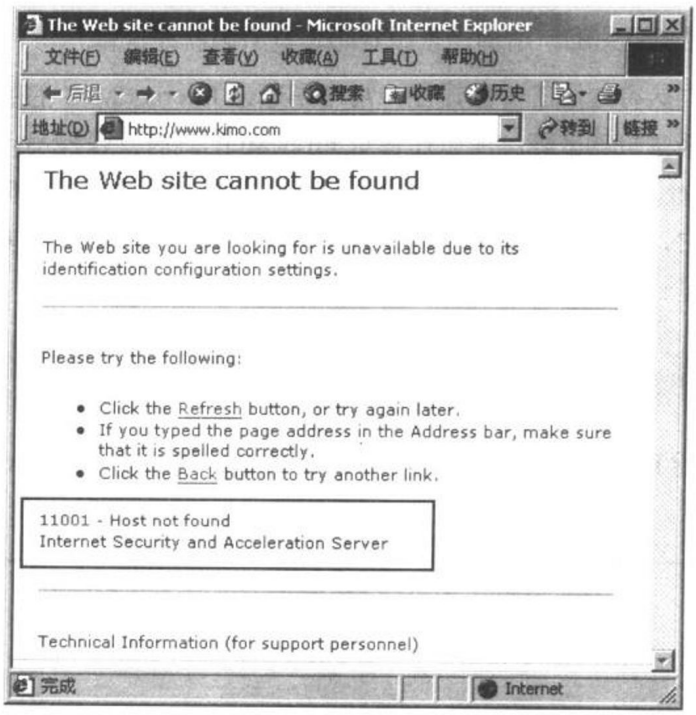


图 1-3 Cache Server 失效时返回的页面

Microsoft ISA Server 2000 所提供的 Cache 机制包含了下列几种功能来加速企业网络的性能：

▶ 内存缓存（RAM Cache）功能：

主要用来减少 I/O 的处理任务，以往代理（Proxy）产品中所提供的缓存，都是使用硬盘内的缓存。ISA Server 2000 中则主要是用内存来加速网站的访问性能。

▶ 主动式缓存（Active Cache）功能：

缓存信息的更新方法主要分为两种：第一种称为“被动式缓存”(Passivity Caching)，这种方式必须在企业内部用户上网浏览数据时，才会将该信息存放在缓存中。第二种方法称为主动式缓存（Active Caching），这种方法根据缓存中数据的有效时间（TTL）设置来判断是否要自动下载更新的内容。无论是被动式或主动式缓存，ISA Server 2000 都有支持。

▶ 可预先调度式缓存（Scheduled Cache）：

ISA Server 2000 中提供有预先调度下载网站数据的功能。这种方式可以由管理员设置让 ISA Server 在网络流量较小的时间点预先下载所指定的网站数据来减少用户连

接 Internet 的时间。

▶ 层次式缓存（Hierarchical Cache）：

这种缓存模式主要是用 Upstream Routing 的访问机制来达到缓存的功能。由最上层的 Cache Server 来决定客户端所提出的要求，决定要从哪一台 Cache Server 来响应。值得注意的是，使用这种缓存模式时需要设置现有企业内部 ISA Server 2000 主机的相关配置。在本书的后续章节中将会提到有关此部份的配置。

▶ 阵列式分散缓存（Cache Array Routing Protocol）：

CARP 用在 ISA Server 缓存客户端与 Web 缓存服务器上。利用 CARP 算法，可以让客户端传送请求到服务器并以阵列的方式存储在服务器中。CARP 使用一个以 smart URL 散列的方式将客户端的请求引导到服务器的阵列里。CARP 允许动态加载平衡、多层次阵列、分布式缓存数据以及在不会有重复内容的情况下增加缓存大小，从而提高缓存命中率和节省带宽。要注意的是：只有企业版的 ISA Server 2000 才提供 CARP 机制，并且需在安装时选择“Multi-Array”的结构模式。读者可参考第 4 章中的“Multi-Array”安装配置流程。

1-3 防火墙的软硬件之分

该如何选择防火墙，以达到最佳的性能价格比？在众多的防火墙产品中既有软件也有硬件，它们之间的差别又在哪里？关于这些问题，笔者可以根据自己的实践经验来为读者简单分析一下。读者可以根据公司内部网络的实际情况来衡量您自己真正的需要。

下面先为读者介绍几款属于硬件结构的 Firewall 的产品介绍：

图 1-4　SonicWall 系列防火墙产品

图 1-4 所示为 SonicWall 系列相关产品，相关参考网址：www.sonicwall.com。

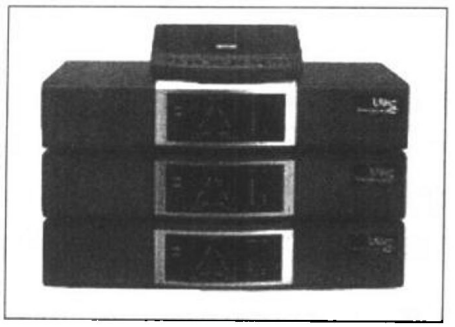


图 1-5　WatchGuard 系列防火墙产品

图 1-5 所示为 WatchGuard 系列相关产品，相关参考网址：www.watchguard.com。

在以上众多的防火墙产品中，除专用硬件结构外就是属于软件的防火墙相关产品了。在这些软件产品中，又分为一般个人用户使用的防火墙软件包和以企业界为导向的企业级防火墙相关软件。现今 Internet 的盛行更应让个人用户在快乐上网时多一层保护才行！硬件与软件的差别，就价格而言硬件 Firewall 产品当然较为偏高，就性能（Performance）而言，则硬件防火墙（Firewall）比较占优势；这个道理与软件模拟的 RAID 硬盘和实际硬件 RAID 硬盘是一样的。

但在这里有一点考虑非常重要，那就是硬件 Firewall 没有 Cache Server 的功能，在市面上所谓的 Proxy Server 相关产品便是包含有 Cache Server 与 Firewall Server 功能的集成应用系统。正因为如此，使得多数的用户会去选用软件的 Proxy Server 相关产品。在 2000 年的 Microsoft .NET 研讨会所强调的企业网络安全管理中，就以 Microsoft ISA Server 2000 作为新一代企业防火墙最佳代表产品。也因为这样，笔者除了在工作中辅导企业界客户应用 ISA 产品外，更想进一步把这实践经验通过此书与所有读者分享。经过上面的简略比较后，相信读者对于防火墙在软件与硬件上的基本差异应该会有初步的认识与了解。

1-4 本书适合的阅读对象

在一个 e 化中的企业团体里，防火墙结构的知识已经不仅仅是 IT 人员本身才需要知道的一门课程，而是企业内部所有客户端用户都必须拥有的基本观念。但是，在选择一套防火墙软件时，IT 管理员关心的是管理界面的使用方便与操作容易。而内部员工关心的是企业网站主机能否多一层安全防护，并加速企业内部客户端对外联机的速度。Microsoft ISA Server 2000 正是根据这种需求发展而来的。下面列出必须学习 ISA Server 2000 的相关人员。

所有企业中的信息主管

一个在企业中担任信息部门主管的人，必须了解许多 IT 业的技术信息，更要让企业在信息化的同时，拥有更快速且更容易管理的信息环境。因此了解及选择最好的防火墙产品，也是担任主管级的人所必须有的责任。

服务于产业界中的网管工程师、MIS 人员

笔者曾经辅导过许多产业界的 MIS 人员，有相当多的 MIS 人员在其公司内部加装 ADSL 宽频网络后都有建立防火墙的需求。主要目的都是希望能够拥有一个简易友好的管理界面，借助它来控制公司内部的网络流量、加速内部用户连接 Internet 的速度，更重要的是保证企业网站信息的安全。

电子商务公司技术部门工程师

网站的安全与此类别的公司可说是密不可分的！想要提供给客户群更好、更稳定的网站服务，其相关的技术人员就必须深入的了解有关于许多网络上安全的技术信息，而学习管理 ISA Server 2000 就是一条最快、最简易的学习道路。

ISP 公司技术人员

目前市面上有太多的 ISP 厂商。然而，如何去选择一个理想的 ISP 服务是每一位用户最想知道的。由于 ISP 服务的客户皆是数以万人以上，因此，提供一个安全稳固的服务是必然的！所以，在 ISP 公司中的网管技术人员更是需要进一步深入的了解有关 ISA Server 2000 的技术信息。

Web Hosting 供货商技术人员

时常听到一些站点信息内容被人通过互联网络侵入窜改的消息。因此，一个提供主机服务的公司必须能够让所有的客户在建立自己公司网站的同时，也能够享有多一层的网站安全防护。所以相关的技术人员就必须学习如何去架构一个具有多层安全机制的防火墙。

所有想要提高自己在 Proxy 技术上的用户

如果，您不是上述几点所提到的相关用户，但是对于有关这方面的技术有相当的浓厚兴趣；或者您正要在您的企业网络中架设防火墙，但却不知从何学起，想要进一步提高自己在这一方面的实力，也可以学习 ISA Server 2000。

如果您是上述成员之一，就可参考这本具有实践经验的管理手册，因为它可帮您省掉许多去研究一些原文数据以及自我模索的时间。总而言之，时间就是金钱！把握每一个学习的机会，就是为自己增添一层竞争的实力。


2
ISA Server 2000 简介

2-1 ISA Server 2000 功能介绍

Internet Security and Acceleration（ISA）Server 是继 Microsoft Proxy Server 2.0 版后的新一版。它除了包含有许多 Proxy Server 2.0 没有提供的服务以外，还强化了前一版的已有功能，这些功能介绍如下：

多重企业阵列策略（Multi-Array Enterprise Policy）

此项功能只有 ISA Server 2000 企业版才支持，它可将最上层的访问策略设置应用到企业内部所有的 ISA Server 主机中。

警报、服务状态、用户连接状态监控（Monitor）

利用 ISA Server 2000 Monitor 可以监控 ISA Server 所有的相关服务状态、警报设置状态、用户连接状态等，一旦出现连接错误或警报信息即可及时处理。

自动产生报表分析功能（Report Jobs）

通过内置的报表功能，即可让管理员设置产生报表分析的脚本。例如：通过每周的报表来分析防火墙在设置上可能产生的缺陷，进而改善。

连接访问策略控制（Access Policy）

通过配置访问策略（Access Policy），可以设置企业内部用户的 Internet 连接权限，以及阻断或允许外部 Internet 用户对企业主机的连接访问。

企业内部网站防护功能（Server Publishing）

过去的 Proxy 2.0 只提供 Web Publishing 的功能，在 ISA Server 2000 中提供了 Server Publishing 机制，可以防护其它类型的 Server，例如：Mail Server 、SQL Server、Telnet Server、Terminal Server 等。

VPN（虚拟企业网络）集成功能

在 ISA Server 2000 中只需简单的设置即可将 VPN 服务与 ISA Server 防火墙作无缝集成。

Security NAT Client 支持

如果您的客户端机器不是采用 Microsoft 相关操作系统，而是使用了其它厂商所提供的操作系统，例如：Linux、OS2、Mac 等。它们无法安装 ISA Server 2000 所提供的防火墙终端（Firewall Client），这时可以使用 Security NAT Client。

预先调度下载缓存功能（Scheduled Content Download Jobs）

预先调度下载缓存功能，可以将企业内部客户端经常连接的网站信息预先下载到 ISA Server 主机，这样一来便可以加速连接 Internet 。

层次式与分布式缓存功能（Hierarchical Cache and Cache Array Routing Protocol,CARP）

在过去 Proxy 2.0 只提供 Hierarchical Cache，在 ISA Server 2000 企业版中为了加强缓存机制的访问性能而提供了 CARP 缓存机制来提高企业版中 Multi-Array 主机的 Cache 性能。

非法入侵检测（Intrusion detected）

黑客的入侵能预警吗？通过 ISA Server 2000 所提供的非法入侵检测（Intrusion detected） 便可以有效的防范黑客的入侵行为。

电子邮件内容过滤（SMTP content filtering）

在 ISA Server 2000 中提供了电子邮件内容过滤功能（SMTP content filtering），让您企业内部拒绝接收所有可能出现问题的邮件。

第三方厂商扩充功能

您想让您所架设的 ISA Server 主机除了拥有防火墙（ Firewall） 与缓存（Cache）机制外，更进一步拥有过滤病毒的功能吗？ISA Server 可以让您加装第三方厂商所提供的防御过滤扩展软件，让您的企业网络更加安全 。

带宽分配功能（Bandwidth Rules）

想自行定义内部客户端以及每一个开放的通讯协议所占用的网络带宽吗？利用 ISA Server 2000 所提供的带宽分配功能（Bandwidth Rules）便可以达到。

软件开发工具（ISA Server 2000 SDK）

如果您对于 ISA Server 2000 现有的功能仍不满意，您还可以利用 ISA Server 2000 所提供的开发工具包自行编写 ISA Server 实用程序。

2-2 ISA Server 2000 客户端的支持

在 Microsoft ISA Server 2000 中，依前端用户的需求不同，分别支持三种客户端的安装方法。