HZ BOOKS

Configuring ISA Server 2000

Building Firewalls for Windows 2000

网络与信息安全技术丛书

配置ISA Server 2000 构建Windows 2000防火墙

附赠 CD-ROM

(美) Thomas W. Shinder
Debra Littlejohn Shinder 著

智慧东方工作室 译

机械工业出版社

网络与信息安全技术丛书

配置 ISA Server 2000
构建 Windows 2000 防火墙

(美) Thomas W. Shinder
Debra Littlejohn Shinder 著
智慧东方工作室 译

机械工业出版社
China Machine Press

ISA Server 是微软公司最新发布的防火墙产品。本书的主要目标是正确布置和配置 ISA，并满足网络安全和网络性能方面的要求。主要内容包括：ISA Server 概述、ISA Server 的企业运行、安全概念和安全策略、ISA Server 配置计划及设计、ISA Server 的安装、ISA Server 的管理等。

本书内容丰富、图文并茂，实用性强。可以使读者迅速掌握 ISA Server 的使用。

本书版权登记号:图字：01-2001-4409

图书在版编目（CIP）数据

配置 ISA Server 2000：构建 Windows 2000 防火墙/（美）辛德（Shinder, T.W.），（美）辛德（Shinder,D.L.）著；智慧东方工作室译. —北京：机械工业出版社，2002.3

（网络与信息安全技术丛书）

书名原文：Configuring ISA Server 2000：Building Firewalls for Windows 2000

ISBN 7-111-09639-8

Ⅰ.配... Ⅱ.①辛...②辛...③智... Ⅲ.计算机网络-防火墙-应用软件，ISA Server 2000 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2001）第 088581 号

机械工业出版社(北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑：周志全 张鸿斌

北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行

2002 年 3 月第 1 版第 1 次印刷

787mm×1092mm 1/16 · 37 印张

印数：0001-4000 册

定价：59.00 元（附光盘）

序　言

——Martin Crasdal（MCSE+I、MCT、CNE、CNI、CTT）
BrainBuzz.com 网站主管

安全问题是每个单位都不敢掉以轻心的。假如一个单位必须以某种形式在 Internet 上“存在”，或者要以某种形式接入 Internet，那么必须对自己进行保护，免受恶意和敌意的入侵与攻击的伤害。

伴随着 Internet 的成长，黑客和黑客工具无论在数量还是质量上都在逐渐发展壮大。那些每天都在上网的单位和家庭用户可以作证，每天都有许多人试图扫描他们的端口或者攻入他们的系统。随着一些廉价高速上网方式的问世，比如 ADSL、Cable Modem 等等，越来越多的人能够“永远在线”，但这同时也增大了遭受攻击的机会。

高速上网也使大量黑客手段变得更易实行。越来越多“傻瓜型”黑客工具的问世，使 Internet 的安全形势变得更加严峻。只要工具在手，即使没有一丁点儿黑客知识，也能轻松地弄垮一台又一台缺乏保护的机器。

为解决这个问题，市面上的防火墙产品也呈爆炸性增长趋势。5～10 年前，只有极少数公司在做防火墙产品，而且大多数产品都十分昂贵，有的得花上万美元才能买到。时至今日，防火墙已成为十分“平民化”的一种产品，各大公司纷纷降价促销。面向几乎每一类上网用户，都有对应的大量防火墙产品可供选择。从普通的家庭用户，一直到大公司、大企业等等，各种层次的用户都有自己“买得起”的产品。

Internet Security and Acceleration Server（简称 ISA Server）是微软最新发布的防火墙产品。初次亮相就效果不凡：在 2000 年底首发的 30 天内，便通过了 ICSA 实验室的防火墙产品认证。如果你熟悉 ISA Server 的前身——Proxy Server 1.0 和 2.0，便会发现 ISA Server 比这些产品又有了明显进步！

ISA Server 是在 Proxy Server 的基础上构建起来的，它吸收了 Proxy Server 的大量优点，并具备其大多数功能，是一种易于扩展的、面向企业级应用的产品，它必然会获得众多公司与企事业单位的广泛接纳。一方面，ISA Server 的安装确实非常容易；但另一方面，它也是一个非常复杂和高级的产品，要求具备一定的知识和技能才能更好地安装和使用。另外，它还是一种会在你的网络基本结构中扮演关键角色的产品。ISA Server 并不是那种在网络中装好后便可以不再管它的产品，也不是那种极易使用、极易实现的一种产品。总而言之，它并非简单地装好并连接好，便能提供我们所需要的一切——真正的 ISA Server 不会让人如此省心！

本书的一项主要目标便是提供真正实用的信息，帮助正确布署和配置 ISA，并同时兼顾在网

络安全和网络性能方面的要求。

1996 年 11 月，微软首次发布了 Proxy Server 1.0。就在那一年的秋天，我已经对这个产品非常熟悉了。因为当年我参加了该产品的首次 T-Preps（培训人员预备课程），考察我是否有资格为其教授正式的微软课程。在这个产品的课堂上，我和其他学员都非常兴奋。在这个产品的身上，我们发现了对一个防火墙产品期待已久的特性，包括回路层和应用层安全等等，同时也亲自体验了内容缓存带来的令人注目的优势。

在那个时候，Winsock Proxy 客户机看起来似乎是一种革命。针对除 Web 页之外的其他 Internet 资源提供“透明”访问时，它工作起来尤其出色。而且只需掌握少量技巧，便能把 Proxy Server 1.0 配置成一个 IPX→IP 网关，所以看起来似乎还是提供高级安全特性的一种出色方案。

不过，这个产品要想真正成为一种网络安全方案，还需要走很长的一段路！尽管 Proxy Server 1.0 确实提供了回路和应用层的安全，但却不支持包过滤和安全警报，也不能提供详尽的日志记录。因此，根本不能把它看作一种防火墙产品，即便它在网络的边界确实提供了某种程度的保护也如此。

对企业用户来说，Proxy Server 1.0 最大的优点在于支持内容缓存，并能控制对网站的访问。通过内容缓存，Proxy Server 1.0 可有效地节省上网带宽，加快访问 Web 的速度。

1996 年，要想以比较“爽”的速度上网，腰包不鼓是基本上不可能的。因此，内容缓存成为颇具吸引力的一种技术，许多单位都愿意用它来缓解上网带宽不足的问题。但在这个领域，即便是 Proxy Server 1.0 这样的微软公司的“大作”，在一些大公司那儿也没有被十分地“看好”。原因很简单，它的缓存系统不能在多个代理服务器中分布，而且在伸缩（扩展）性能上也不是特别理想。

面对 Proxy Server 1.0 的种种不足，微软很快做出了反应，并在 1997 年发布了 Proxy Server 的 2.0 版本。Proxy Server 2.0 引入了早期产品缺乏的一些特性。最起码，新产品支持动态包过滤技术。这是一种十分强大的网络保护机制——只有在真正需要通信的时候，它才会自动打开端口，建立与 Internet 的通信连接。换言之，管理员没有必要亲自打开静态包过滤器来允许访问。

Proxy Server 2.0 还提供了多种实时警报，可在发现网络入侵企图时及时地通知管理员。对 SOCKS 的支持也是新加进来的，它主要面向那些非微软的客户机（比如 UNIX 工作站）。对这部分客户机来说，即使没有安装 Winsock 代理，也并不一定只能使用与 CERN 兼容的 Web 浏览器来访问因特网。Proxy Server 2.0 还支持内部 Web 服务器的动态发布，而且也能进行服务器代理。通过这种功能，Internet 上的用户便可访问内部网络中运行的大多数服务。

和以前的版本相同，Proxy Server 2.0 也支持内容缓存。不过在新版本中，微软对这一功能做出了多处明显的改进。现在的内容缓存可扩展到在多台服务器之间进行，要么采用分布式缓存机制（distributed caching），要么采用分级式缓存机制（hierarchical caching）。通过分布式缓存，管理员可将缓存分布到由多台服务器组成的一个阵列中，而且在每台缓存服务器之间，不会出现任何内容重复的现象。缓存阵列不仅具有容错能力，而且还具有负载平衡的特征。

通过分级式缓存，管理员可将代理服务器连接到一条内容缓存链中。对那些设立了分支机构的大型公司来说，分级式缓存是最理想的。假如分公司的 Proxy Server 没能在自己的缓存中找到

需要的内容，那么内容请求稍后就可路由至总部运行的 Proxy Server，看看那里有没有自己需要的内容。另一处明显的改进便是增加了主动缓存机制，它使 Proxy Server 在服务器相对处于空闲的时候对缓存中经常访问的对象进行更新。这样可进一步改进缓存的性能与质量。

然而，尽管做出了这些改进，Proxy Server 2.0 仍然不算是最完美的，依然遭到了许多批评。至少有一点需要提醒大家注意，在某些情况下，Proxy Server 2.0 真正运行起来非常困难，而且还可能有一点儿不可靠。举个例子来说，要想让自己的内部 Exchange 服务器接收来自 Internet 的邮件，那么必须在 Exchange 服务器上安装 Winsock Proxy，然后配置一个 WSPCFG.INI 文件，在 Proxy Server 的外部接口上为 SMTP 通信绑定一个正确的监听接口。

经过一系列复杂的操作，Proxy Server 终于能代表内部的 Exchange 服务器对 SMTP 请求进行监视。但事情还没完，你还必须在 Exchange 和 Proxy 服务器之间一直保持一个有效的控制通道。假如这个通道由于某种原因而失去了，便无法接收任何 SMTP 邮件。而在丢失了控制通道之后，为了重新获得 SMTP 能力，惟一的办法便是重新初始化服务，或者重新启动计算机。尽管像这样的情况并不是经常出现，但许多人仍然强烈建议不要在一个大规模应用环境中采用 Proxy Server 2.0——假如你不想为 SMTP 服务而劳神的话。

另外，Proxy Server 2.0 有一个非常著名的“缺点”便是没有获得 ICSA 实验室的防火墙产品认证。正是由于 Proxy Server 2.0 没有获得 ICSA 实验室颁发的合格证书，所以许多人推断它不是一个能提供真正网络防护的防火墙产品。然而，这样的推断是不客观的，对 Proxy Server 来说也是不公平的。

Proxy Server 2.0 之所以未能通过 ICSA 实验室认证，不是它提供的安全能力不够，而是它要求采用一个专利性的客户机软件（比如 Winsock Proxy 客户机）为某些服务提供进入和外出通信。但是，ICSA 认证标准对此有着严格及清楚的规定：不允许使用特殊或专利客户机软件为某些指定的协议提供进入和外出访问，这些协议包括 DNS、SMTP、HTTP（S）、TELNET 和 FTP 等。

但不管怎样，正是由于未通过 ICSA 实验室的认证，所以极大地影响了 Proxy Server 2.0 的销售。许多公司在自己的采购政策中都明确规定：除非通过了 ICSA 认证，否则根本不予考虑！后来当 ISA 发布的时候，假如你留意过和它有关的新闻组文章，便会发现人们问得最多的一个问题便是：“ISA Server 通过了 ICSA 认证没有？”

幸运的是，ISA Server 在 2001 年 1 月通过了 ICSA 实验室的认证。自产品发布到通过认证，微软的动作通常都是挺快的，这一次的 ISA Server 也不例外！正是由于 ICSA 的证书在握，而且人们普遍认为 ISA Server 能提供和通过 ICSA 认证的其他产品一样等级的安全防护能力，所以 ISA Server 有可能具有比 Proxy Server 2.0 更高的市场接纳度。

但应该注意的是，为了对 ISA Server 进行有效的配置，令其符合面向防火墙性能的 ICSA 3.0a 标准，我们必须采取诸如禁止 Web Proxy 服务这样的操作。针对 ISA Server 的配置，本书提供了大量信息，可帮助重现真正符合 ICSA 实验室标准的配置。

任何人即便只是草草地浏览一下 ISA Server，也会发现它和 Proxy Server 2.0 完全是两种不同的产品。尽管它的部分特性和 Proxy Server 2.0 相同，比如两者都通过动态包过滤器以及缓存阵列协议（CARP）来实现分布式缓存阵列，但是，ISA Server 引入了大量新特性，做出了大量改

进，而且采用了一套全新的管理界面。

另外，ISA Server 提供了两个版本：标准版（Standard Edition）和企业版（Enterprise Edition）。其中，价廉物美的标准版是一些小公司的理想选择，这些小公司既不需要用多台服务器来组成一个缓存阵列，也不需要通过 Active Directory 来控制企业级的阵列策略。而较大的公司可考虑购买更昂贵的企业版，以便利用一些同 Active Directory 集成到一起的中心控制策略。

另一处显著的改进是 ISA Server 支持 SecureNAT（安全网络地址翻译）。这意味着不需安装 Winsock Proxy 客户机，即可通过 ISA Server 来使用除 HTTP（S）和 FTP 之外的其他协议。由此造成的直接效果，便是为自己的 Macintosh 和 UNIX 客户机提供 Internet 访问时，不再需要专门对 SOCKS 进行配置。

换言之，ISA Server 对 SOCKS 的支持变得更加精简。不过，这并不是说 SOCKS 支持是可有可无的。尽管不再需要安装防火墙客户机来提供对 Internet 资源的访问，但有时仍然需要安装它，以便按用户或用户组的名字对外出的访问进行控制。

本书将花费大量笔墨，向大家解释把内部计算机配置成 SecureNAT 或防火墙客户机的优点与缺点。同时，还会解释每一种客户机适合用在什么样的环境中。

与 Proxy Server 2.0 相比，为内部 Web 服务器和其他服务提供访问的方式也发生了极大的变化。现在有一些特殊的向导可供发布 Web 和 Mail 服务器。现在的服务器发布是通过 SecureNAT 来完成的。服务器发布不再要求我们必须在一台内部服务器上安装 Winsock Proxy，也不再需要配置一个 WSPCFG.INI 文件将恰当的端口同 ISAServer 上的一个外部接口绑定起来。不过，ISA Server 仍然支持这种形式的服务器发布，以保持向后兼容。同时，利用这种形式，也可发布那些要求使用辅助连接方式的应用程序；否则的话，便必须为其使用一个应用程序过滤器（application filter）。

ISA Server 还配套提供了数量众多的应用程序过滤器，用于为大量协议提供进入和外出访问控制。其中包括用于控制 FTP 数据传输的应用程序过滤器，也包括用于 SMTP、HTTP 重定向、DNS 入侵侦测、流式媒体和 H.323 的应用程序过滤器。其他还有许多，这里不再赘述了，正文中有详细描述。

注意，ISA Server 提供了一个所谓的“H.323 网闸”（H.323 Gatekeeper）以及“H.323 网关”（H.323 Gateway），用于为兼容 H.323 标准的客户机（比如 NetMeeting）提供注册和呼叫服务。通过 H.323 网闸和网关，NetMeeting 客户机可在内部网络以及 Internet 上使用完全的音频和视频能力相互间进行通信。来自 Internet 上的呼叫也可以转接到内部的 NetMeeting 客户机——只要它在网闸那里进行了注册。

要真正理解和配置这些组件，许多管理员恐怕又得头疼好一阵子了。不过幸好有了本书。本书通过大量实例，对 H.323 组件的配置进行了清晰地解释。事实上，就在写作本书的时候，ISA Server 的 H.323 功能便帮了我们很大的忙，我们用它来实现“内部通话”。

与 Proxy Server 2.0 类似，ISA Server 能用来支持 VPN（虚拟专用网）。不过，ISA Server 使内部客户机能够连接到 Internet 上的 VPN 服务器。这对许多人来说都是一个期待已久的功能。另一个重要的改进是 ISA Server 提供了大量有用的向导，能引导我们逐步完成 VPN 的配置。举

个例子来说，假如想建立与一个远程 ISA Server 的“即需即拨”式 VPN 连接，那么便会有相应的 VPN 向导帮助我们简单、直观地完成整个设置过程——再也不必像以前那样为此而大费周折了！事实上，同路由和远程访问向导相比，ISA Server 的向导意味着一次巨大的进步。

在本书中，既有丰富的理论解释，也有实战性的操作步骤，指导各式各样的 ISA Server 配置。值得注意的是，尽管许多向导（特别是 VPN 向导）可极大简化 ISA Server 的配置与管理，但对于理解它们背后的基本原理来说，却是没有多少帮助的。一名真正的管理员不仅要知道如何操作，更重要的是理解为什么要这么操作。

利用“向导”这个好东西，人们只需通过一系列简单的步骤，便可成功地完成特定的配置。但在绝大多数情况下，人们（特别是管理员）都应该站在全局的高度，仔细地考察自己的每一个步骤。换言之，每个步骤都不应单独地看待，而应该把它放到一个概念性的整体中，考察它的前因后果。这样做有助于理解自己“为什么”要采取一个特定的操作，并且围绕自己的任务目标，客观地评价这个步骤。在设计本书的步骤指南时，我们正是朝着这个方面努力的。我们会提供足够多的解释，帮助读者去深入理解自己的产品，同时习惯于通盘地考虑一个问题，认清自己的每一步行动的后果，以及为什么要采取这一行动。

本书兼顾了有经验和没有经验的管理员。因此，针对一些比较重要的主题（比如安全性），这本书里提供了大量背景知识介绍。比如第 3 章解释一些重要的、相互关联的安全性概念。在这一章中，可学到什么是“欺骗”，以及 Smurf 攻击具体是怎样来实现的。另外，由于作者本身便具有极其专业的法律知识，所以除了纯粹的 ISA Server 配置技术之外，读者还可从中学到足够多的、其他方面的安全防范常识。

防范自己不受所谓“社交工程”（Social Engineering）的侵害是至关重要的。在别人花言巧语面前，请不要掉以轻心！对此，一个非常经典的例子便是 Versign 公司的工作人员由于不小心，被别人骗走了微软公司的数字证书。针对防火墙的设计和管理概念，本书也提供了非常好的背景知识介绍。举个例子来说，作者在防火墙的环境中，为美国国防部采用的 TCP/IP 和 OSI 模型提供了详尽的解释。通过这些解释，有助于澄清同防火墙有关的关键术语，比如“回路过滤”（circuit filtering）和“应用程序过滤”（application filtering）等等。

在自己的网络上安装和实现 ISA Server 并不是一件轻而易举的事情。只有在经过深思熟虑之后才能“动手”，切不可草率而为。本书提供了大量信息来帮助读者展开并配置自己的 ISA Server，使你能真正从网络提供的安全与性能增强特性中获益。由于 ISA Server 适用于各种规模的网络，所以本书也提供了相应的信息，帮助读者拟定相应的计划，将 ISA Server 安装成一台单机式服务器，或者安装成一个企业阵列（Enterprise Array）。本书还涉及了集中和分布式管理的主题。

本书的厚度反映了 ISA Server 的复杂性，也反映了我们认为有必要提供的信息量大小。稍微浏览一下本书，便会发现它的章节组织非常有条理，对于该产品的方方面面均进行了彻底的、详细的解释。

第 1 章对 ISA Server 的特性进行了一番概述，然后讨论了它作为一款企业级产品理应具有的扩展能力。该章还详细讲述了 Active Directory 的概念。第 2 章对安全方面的主题进行了详细讨论。随后的一章则解释了如何计划 ISA Server 的安装，其中同时探讨了在硬件和基本结构方面的

一些考虑。

有些时候，人们需要在用于安装 ISA Server 的那台 Windows 2000 Server 机器上计划一个安全配置。因此，我们提供了详细的信息，讲解如何做好一些准备性工作——比如如何在外部接口上禁用 NetBIOS——以确保服务器具有最大程度的安全性。另外，我们还详细解释了各种磁盘方案（比如 RAID 5）的优缺点，在各类中立区或非军事管制区（De-Militarized Zones，DMZ）中如何配置 ISA Server，以及如何将 ISA Server 同 Active Directory 集成到一起等等。

在第 5 章，我们开始讲解安装 ISA Server 的具体细节。如同本书的大多数内容一样，这一章会深入浅出地解释各项选择的含义，解释 ISA Server 的安装与配置有关的大量细节。

后面的章节介绍与许多主题有关的信息，其中包括如何从一个 DMZ 和内部网络中发布服务，如何配置日志和警报，如何自动配置客户机，如何设置 VPN，如何设置路由选择，如何安装数字证书等等。事实上，本书会一步一步引导大家学习和 ISA Server 的几乎每个接口有关的选择，同时提供大量有用的信息，帮助读者判断哪一种配置才是最恰当的。

尽管本书涉及内容广泛，但是，应该强调哪些内容和例子都是经过精心考虑的。自测试版开始，我们便接触并使用这个产品，而且每天都要和新闻组上的大量用户打交道，倾听他们的意见，并据此做出最正确的选择，所以我们在本书提供的都是大家最关心的、第一手的资料。比如在我们讨论服务器发布的时候，大家便能详细了解如何设置自己的 Outlook Web Access，还会了解到与 DMZ 的设置和配置有关的细节。另外，读者还会找到许多有用的故障诊断信息，所有这些信息都来源于我们自己和其他一些人的实际经验，可通过它们解决实际工作中有可能遇到的几乎任何问题。

无论你是才接触防火墙和代理服务器的新手，还是已经拥有了大量的经验，在你计划、安装、维护和调试 ISA Server 的时候，我们都希望并相信这本书能够对你有所帮助。在此，作为本书的技术编辑，希望大家能够和我一样，被作者在 ISA Server 2000 上的深厚功底所折服，被这本权威的、全面的以及实在的参考书深深打动！

目　录

第 1 章　Microsoft ISA Server 入门

本章要点：

- 什么是 ISA Server
- ISA Server 特性一览
- 本书面向的读者和涵盖的内容

1.1　什么是 ISA Server

在 IT（Information Techonlogy，信息技术）的世界里，随处都充满了大量的缩略语；有的人甚至把这一情况戏称为“语言的改造”。有的时候，缩略语也未免太多了一点儿——它们代表了如此多不同的概念、产品、组件和协议——甚至让我们怀疑是否有一天会用光所有的字母组合。身在 IT 世界，你会发现早期采用的许多缩略语现在都被赋予了崭新的含义。

因此，我们在此需要郑重声明：在这本书中，ISA 不是“工业标准结构”（Industry Standard Architecture，ISA）总线。ISA 总线是许多老一代 PC 迷所熟知并热爱的东西，老式的计算机接口卡采用的便是 ISA 总线标准。而且，本书的 ISA 也不是“仪器、系统和自动化社会”（Instrumentation, Systems, and Automation Society，ISA），那不过是一家专业组织，主要面向的是测量和控制技术。本书的 ISA 是指由美国微软（Microsoft）公司发布的又一款服务器产品（或者更准确地说，是为以前的一个老产品赋予的新名字）。

微软发布了新一代的、面向商务的操作系统——Windows 2000——之后，马上便宣布会接连推出几款新的服务器产品，要么在基于 Windows 2000 的网络中提供新的功能，要么对以前在 Windows NT 4.0 上运行的那些附加服务器产品做出改进。

随着时间的推移，微软的承诺一一兑现。我们接连看到了 Exchange 2000 和 SQL Server 2000 等服务器升级产品，它们都引入了大量崭新的功能，而且都能同全新的 Active Directory（活动目录）紧密集成。至于一些全新的服务器产品，比如 Microsoft Mobile Information 2001 Server 和 Microsoft Application Center 2000 Server 等，也在积极地开发当中，并承诺会充分迎合最新的 PC 计算潮流，比如支持无线连网和应用程序服务供应商（ASP）等等。对微软一些原有的服务器产品（比如 SNA 和 Site Server 等等）来说，则纷纷更换了一个更时髦的名字，比如 Host Integration Server（主机集成服务器）和 Commerce Server（商务服务器）等等，以反映出它们想重点强调的新特性。

另外还有一个产品也得到了一个新名字，这便是本书的主题，微软针对 Web 缓存、过滤和连接共享而设计的软件包：Proxy Server。对这款产品的 Windows 2000 兼容版本来说，它开发时采用的代码名为 Comet，但等最终发行时，却变成了“Microsoft Internet Security and Acceleration

Server 2000”（微软 Internet 安全和加速服务器 2000）。另外，也可更简单地称作 ISA Server 或者 ISA Server 2000，如图 1-1 所示。

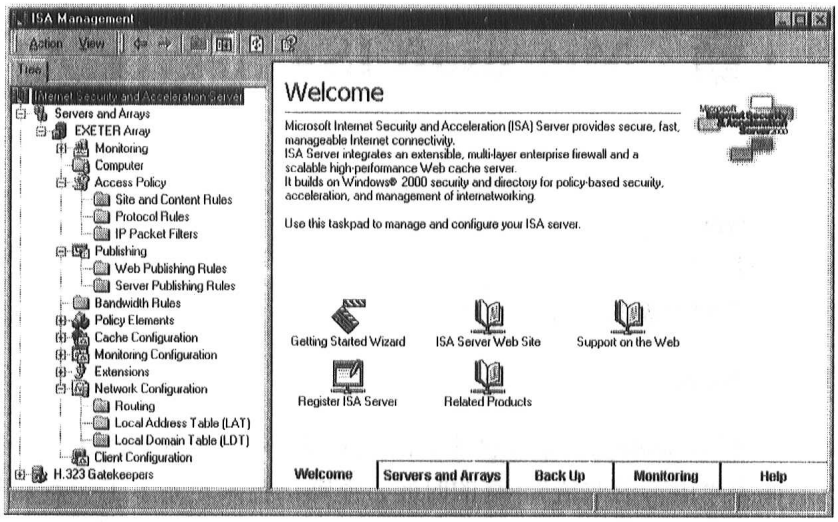

图 1-1　微软的 Internet Security and Acceleration Server 2000（ISA Server 2000）具有与 MS Proxy Server 类似的特性——同时还进行了大量改进

1.1.1　“安全和加速”的来历

嗯，“Internet 安全和加速”。听起来似乎不错，但到底是什么意思呢？在本节，让我们首先来认识一下它的两个重要元素：安全和加速。然后，探讨一下各自在 ISA Server 中扮演的角色，并解释它们为何对一个网络来说是至关重要的。

与以前的 Proxy Server 相似，ISA 实际上也提供了两大系列完全不同的功能。有的单位主要使用 ISA 的安全特性，对内部网络进行保护；有的单位则主要利用它的加速特性。当然，更多的公司则同时利用了这两方面的特性。

1. Internet 安全

在计算机连网的早期岁月里，安全问题只有某些政府机构和大公司才会考虑。普通中小型公司根本没将安全问题放在首位。至于原因，不外乎是“我们的计算机根本没什么东西可偷”或者“我们已经有了一个安全的网络——只有输入密码才能进入”等等。

现在看起来，这些理由当然都显得十分天真和可笑。不过抛开这一切不谈，几年前，确实有许多计算机不必像现在这样关心安全问题，这主要是由以下几方面的原因造成的：

- 以前计算机和网络设备显得过于昂贵，绝对不像现在这样普及。因此，即使在一家大公司里，也并不是所有计算机都有必要连网的。
- 单位里只有极少的信息采用数字格式保存，所以极少有资料会在网络上出现的——即使那个网络确实连到了“外部世界”。
- 在 20 世纪 90 年代之前，许多公司的网络都是一种封闭式系统。计算机被统一连到一个“站点”之内（都在一个局域网中），以共享公司内部的资源。此外，一些较大的公司甚

至采用了专用线路，把自己设在不同地理位置的分公司连接到一起。但无论如何，只有最大和最爱赶时髦的公司才拥有进入全球“公共”网络的连接。在那个时候，Internet 主要由教育和政府系统的人员使用。即使一家公司确实能够进入 Internet，也往往只通过拨号方式“上网”，根本不像现在这样普遍都能“永远在线”。因此，外部人员如果想侵入公司的内部网络，会觉得十分困难。

- 由于只有极少数人才能接入 Internet，所以只有非常少的人才会产生刺探公司数据的想法（无论是为了获利，为了报复，还是只为了“有趣”），而只有更少数的人才真正拥有相应的工具和手段。
- 实现一个“防火墙”（安全保护）通常十分复杂，而且代价高昂，要求购置新硬件以及难以操作和维护的软件。
- 极少有什么法令和其他法律条款要求公司采取安全防护措施来保护自己的机密数据。

（1）时代在变化，安全问题也越来越重要

进入 21 世纪之后，越来越多的公司——甚至还有大量家庭用户和非赢利性组织——都把自己的计算机连成了网络，并接入全球性的 Internet。通过这种世界范围内的计算机网络化，人们可以访问以前从未见过的海量信息，也使得大量工作更易开展——不过同时也带来了一系列弊病。

从理论的角度说，假如你的局域网（LAN）内的用户能够访问遍及全球的计算机，那些计算机的用户或许也能够访问你的计算机。毕竟，连接是双向的，如果你不采取措施保护自己的内部网络，那么一名普普通通的黑客就能访问你保存在网络服务器中的文件，复制机密数据，甚至植入病毒，或者删除你的硬盘数据等等。

另外，并非仅仅“机密”数据才需要保护。有的网络管理员认为安全问题无关紧要，因为自己网络中的数据并不是“机密”数据。在此请大家注意，数据的“完整性”一样需要保护。对一套安全方案来说，它的目的并不仅仅在于阻挡闯入者访问机密数据，还要保证重要的数据不被破坏或更改。

设计与计划：安全威胁和安全方案

对一套全面的安全方案来说，它必须能应付各种类型的安全威胁。对自己的网络实行安全保护时，请记住几个方面的因素都得强调。设计自己的总体安全计划时，它应该能够进行下面这些保护：

- 敏感数据必须保密。
- 敏感和非敏感数据的完整性。
- 网络的正常运行（防范由于病毒或直接入侵而导致系统文件被恶意破坏）。

安全方面的威胁表现在多个“层面”上，但主要还是可以分为两大类别：外部威胁和内部威胁。举个例子来说，由黑客在一个远程地点发起的“拒绝服务”（DoS）攻击是一种外部安全威胁，而公司员工误删重要文件则属于内部安全威胁。从表面上看，似乎 ISA Server 只保留我们不受来自外部的侵害——阻挡那些自 Internet 发起的对你的 LAN 的进攻。不过，ISA 事实上也允许我们限制从 LAN 发出的对 Internet 的“外出访问”。