亨达科技 李静安 编著

高级防火墙

高级防火墙

ISA Server 2000

本书特色

整合防火墙与防毒墙，打造安全无虑的网络环境

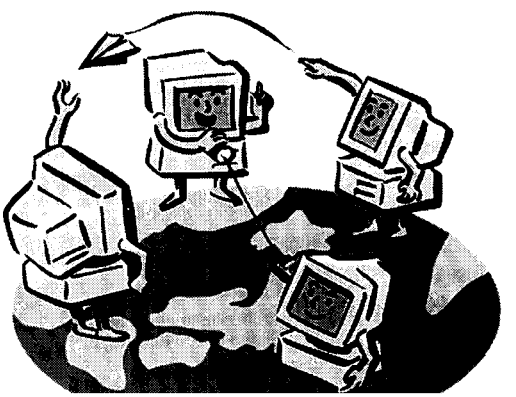
- 认识ISA Server，以及它在.NET平台的定位
- 如何规划与部署企业网络，有效管理客户端
- ISA Server的安装步骤演练，以及安装后的通讯测试
- ISA Server的七项策略元素说明
- 抽丝剥茧地介绍防火墙的管理与设置
- 实例说明Cache的管理，并深入设置的核心
- 图文并茂的性能监视与报表管理，说明系统的维护、服务与管理
- 升级Proxy Server 2.0至ISA Server的注意事项与考虑
- 架设防毒墙与防火墙，捍卫企业网络安全

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

高级防火墙

ISA Server 2000

亨达科技 李静安 编著



中国铁道出版社

2002 年 · 北京

（京）新登字 063 号

北京市版权局著作权合同登记号：01-2002-0275 号

版 权 声 明

图书在版编目（CIP）数据

高级防火墙 ISA Server 2000 / 李静安编著 —北京：中国铁道出版社，2002.1

ISBN 7-113-04550-2

Ⅰ.高… Ⅱ.李… 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(2002)第 005614 号

书　　名：高级防火墙 ISA Server 2000
作　　者：亨达科技 李静安
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）
责任编辑：苏茜 郭毅鹏
特邀编辑：徐煜东
封面设计：孙天昭
印　　刷：北京兴顺印刷厂
开　　本：787×1092　1/16　印张：17.75　字数：428 千
版　　本：2002 年 2 月第 1 版　　2002 年 2 月第 1 次印刷
印　　数：1～5000 册
书　　号：ISBN 7-113-04550-2/TP・676
定　　价：27.00 元

出 版 说 明

Microsoft ISA Server 2000 是微软推出的第一套正宗的防火墙，原名为 Microsoft Internet Security and Acceleration Server 2000。本书将完整介绍 ISA Server 的建置、部署与安装、操作。一扫以往大家对防火墙的印象：

- 安全上：除了可以保障企业与网络的安全外，还可以自行开发或向相关周边厂商购买外挂程序，对外新的攻击方式或系统问题，微软仍会不断提供更新程序，这就是所谓的 Service Pack（服务包）。
- 价格上：微软的产品价格，一向都是大众化价格，一般公司也能够接受。
- 技术上：看完书后，你应该有足够的能力可以自己架设一个防火墙。

本书由台湾学贯行销股份有限公司提供版权，经中国铁道出版社计算机图书项目中心审选，张巍、王秀平、张迈、廖康良、陈贤淑、孟丽花等同志完成了本书的编排工作。

2002 年 2 月

目　录

第一章

综观 ISA Server 2000

1-1 ISA Server 简介

1-1-1 ISA Server

现在已经很难找到没有网络（Network）的大企业或小公司，不论是局域网（Intranet）还是互联网（Internet），架设网络都已经是必要的装备之一，但会对网络做安全防护的人却不多，本书将介绍 Microsoft Internet Security and Acceleration Server 2000（以下简称 ISA Server），ISA Server 是目前在 Windows 2000 Server 平台上唯一同时具有“防火墙”与“网站缓存”的服务器软件，一次解决网络上黑客横行的安全问题与带宽不足的速度问题。

ISA Server 与 Windows 2000 Server 在系统上有许多紧密的结合，也大幅提升整个网络上传输数据的安全与速度。安全上有“多层次的防火墙”可以有效阻挡黑客及任何未授权者的进入，速度上有“高效率的网站缓存”让用户拥有更快的网络传输速度，另外，还有集中式直觉化的管理界面、使用简单、多样化的报表系统、管理性能的提升，最重要的是，ISA Server 降低了网络复杂性与成本。

1-1-2 Dot NET 与 ISA Server

很多人听说过.NET，但是说不出.NET 是什么！简单一句话解释，Microsoft＝.NET；微软的.NET 平台将彻底改变人与计算机之间交互的方式，也就是“人”不需要担心如何与“计算机”交互的问题，.NET 最终将实现让所有用户可以在任何地方、利用任何装置，来获得用户的数据或应用服务的愿望，譬如：用户可以经由手写输入、语音辨识或视觉技术来与数据间达到交互效果，数据会安全的储存在互联网上，用户可以随时从公司或家里的计算机、移动电话、PDA 等装置，达到实时传递数据或信息的目的，而.NET 最后要做到的是“商业无国界”的境界。

Microsoft 在.NET 中将 Back-Office 系列转换成现在的“.NET Enterprise Servers”系列产品（如图 1-1），是一整套完整的企业应用服务器，而且全部都以 Windows Server 2000 为平台，其中的成员如下：

- ISA Server 2000：高级防火墙及高效率的网络缓存服务器。
- Application Center Server 2000：建立服务器集群，有效达到负载平衡及增加容错转移与延展性。
- Exchange Server 2000：全方位的信息交换及知识管理平台。
- SQL Server 2000：最完整的关系型数据库及分析系统。
- Commerce Server 2000：快速构建高效率的 B To C、B To B 等商务系统。
- Biz Talk Server 2000：利用 XML 及 SOAP 等技术，达到与远程的客户系统的数据交换或信息沟通。
- Host Integration Server 2000：整合非微软平台的数据来源与沟通。

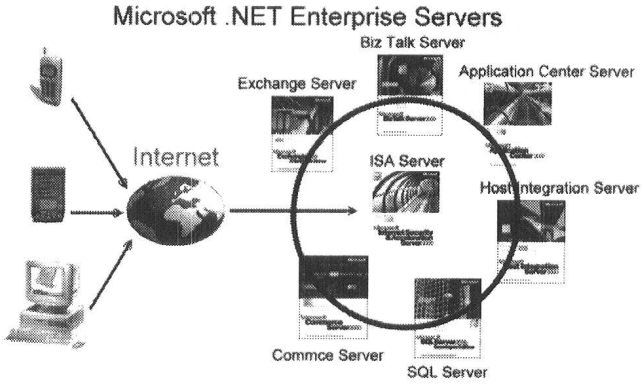


图 1-1 .NET Enterprise Servers 系列产品

Microsoft .NET Enterprise Servers 共包含以上七套应用服务器产品，各有各的专业空间，惟安全整合问题，多半交由其公用平台 Windows Server 2000 处理，但对整个网络来说，安全问题全部交由 Window Server 2000 处理，但还是有一些不足，尤其缺少整个网络的“门禁管制”（也就是一般所谓的“防火墙”），ISA Server 整合 Windows Server 2000 形成一道安全屏障，所以在.NET Enterprise Server 群里，ISA Server 实为安全上最重要的一套应用服务器。

1-2 ISA Server 版本介绍

1-2-1 版本介绍

Microsoft ISA Server 2000 的前身是 Microsoft Proxy Server 2.0 版，Microsoft 推出.NET Enterprise Servers 时，将 Proxy Server 更名为 ISA Server，目前提供“标准版”、“企业版”、“升级版”三种版本。

ISA Server 标准版

ISA Server 标准版提供了企业级的高级防火墙、网站缓存能力、直观式的管理模式，适用于中小型企业组织、工作组等环境。

ISA Server 企业版

ISA Server 企业版设计的目的是用来满足一些网络高流量要求，诸如高性能、容易管理、大量网络用户、多层次的访问策略、高度容错能力的企业网络环境，除了标准版的所有功能外，企业版主要可以架设多台服务器形成阵列模式。

ISA Server 升级版

ISA Server 升级版里又区分为“标准版”、“企业版”两种，以 Microsoft Proxy Server 2.0 版升级为主，但是 Proxy Server 1.0 不能直接升级至 ISA Server2000。

1-2-2 版本的差异性

ISA Server“标准版”与“企业版”具有某些相同的特性，譬如：同等级的防火墙功能以及强大的网站缓存功能。

ISA Server“标准版”最多支持到 4 个处理器（CPU），若需要更多的 CPU 服务器主机、服务器阵列或多层次网络部署策略等，就必须使用 ISA Server“企业版”。“标准版”与“企业版”的差异性如下表：

表 1-1

项　目	标 准 版	企 业 版
防火墙	相同	相同
网站缓存功能	相同	相同
管理模式	相同	相同
服务器部署模式	独立式（Standalone）	独立式（Standalone）/多服务器模式（Array）
管理等级	本地端（Local Network）	阵列式可跨网络
处理器限制	最多 4 个 CPU	无限制
层次式缓存	层次式缓存	层次式缓存/分布式缓存
Active Directory	如果安装 Standalone 模式，ISA Server 的系统信息将存放在登录编辑文件（Regedit）中，如果安装 Array 模式，ISA Server 的系统信息将存放在 Window Server 2000 的 Active Directory 中，所以安装 Array 模式的第一台 ISA Server 主机，必须是一台网域 DC（Domain Control），第二台 ISA Server 必须是网域的 Member Server 主机，相关说明会在第 2 章企业网络规划中详细叙述。	

注：如果你不知道 AD（Active Directory）、DC（Domain Control）、Member Server，请参阅 Window Server 2000 相关书籍中 Active Directory 部分。

1-2-3 产品授权

ISA Server 的授权及售价方式，是以处理器（CPU）的数目来计算：

- 每一台服务器的每一个处理器（CPU），都需要取得一个使用授权，至于售价请参考微软的网站或经销商网站。
- 每一个使用授权，包含不限量的用户连接，不论内部的局域网（Intranet）或是外部的广域网（Internet），不需要再购买额外的服务器授权、客户端访问授权(CALs)或是互联网连接授权。

1-3 安装环境

1-3-1 系统需求

要使用 ISA Server，你的系统环境必须达到以下要求：

- 系统安装 Windows 2000 Server 版，并升级到 Service Pack 1 以上或 Windows 2000

Advanced Server 版，并升级到 Service Pack 1 以上；或安装 Windows 2000 Datacenter Server 版。

- Pentium II 300MHz 或以上的 CPU。
- 256 MB 以上的 RAM。
- 20 MB 以上的可用磁盘空间。
- 必须有一个 NTFS 的硬盘分区，最好有 100MB 以上。
- Windows Server 2000 兼容网卡，一般规划为两块网卡，一块用在内部网络连接，另一块用在外部网络连接。
- 若要构建 ISA Server 阵列（Array）规划，还需要安装 Windows Server 2000 的 Active Directory 在网络环境。

1-3-2 环境需求

ISA Server 本机必须安装在 Windows Server 2000（SP1）平台上，不可以安装在 Windows NT 4.0 平台上，如果现有内部网络的环境是 NT 网域时该怎么办？

如果安装 Standalone 模式，内部网络可以是 NT 网域环境；如果安装 Array 模式，至少必须有一个 Windows Server 2000 网域环境（可与 Windows NT 4.0 网域共存），而且每一个 Array 成员必须是 Windows Server 2000 网域的会员服务器（Member Server）。

1-4 ISA Server 的特色

ISA Server 整合了许多强大的功能，并提供网络上性能的提升与安全的保障，为了让安装 ISA Server 之前，能更了解它的重要特色，整理出六大项目，说明如下。

1-4-1 多层防火墙与安全的特色

当你在一个企业网络的门口装上 ISA Server 时，网络内部用户在使用网络时，并不会察觉防火墙正在从中进行筛选的操作，因为速度及任何应用都不会改变，除非内部用户想连接被管理者设置拒绝访问的站点。ISA Server 防火墙的安全运行，有以下几种处里方式：

包过滤（Packet Filtering）

当你设置 IP 包过滤功能来让部分指定的包才能通过 ISA Server 时，就已经为你的服务器建立了安全的保护，譬如：冻结由内部网络前往外界网络非法站点的数据流，或冻结 Internet 上由某些特定主机发出的数据流，也可以自行制定包过滤的规则（Rule）与策略（Policy），过滤内容大致如下：

- 服务类型，如：Telnet、Mail、News 等。
- port 号码。
- 内部用户计算机或外部目的地（远程）计算机名称（Host）。
- 其他非包的过滤规则。

IP 包过滤功能，是属于“静态的筛选”，意思是针对指定的 Port 做检查的操作，ISA Server

还支持“动态包筛选”（Dynamic Packet Filtering）功能，即 Port 只有在需要通讯时才自动的打开，在结束时自动的关闭，这样的方式可以把外露的 Port 减到最少，自然会更安全。你也可以冻结 Port 区段以及检测包层次的攻击行为。

应用程序过滤（Application Filtering）

ISA Server 支持几乎所有网络上的应用程序，譬如：HTTP 网站、FTP 文件传输、TELNET、多媒体程序、SMTP 邮件传输、在线会议等，并对其包作查看、监督、冻结、修改与重新导向等操作。

除了安装 ISA Server 时预设的几个常用应用程序过滤器以外，还可以自行开发（SDK），或向相关厂商购买其他应用程序过滤器使用与扩充。

入侵检测（Intrusion Detection）

自定义警告来提醒有不明的入侵者，以及当入侵发生时要作出反应，包括发 E-Mail 或呼叫管理者、停止服务器运行、写入系统日志或执行某个解决程序等，现在常见的入侵工具软件，如 Port Scanning、WinNuke 和 Ping of Death 等，ISA Server 都可以有效的防止，并能检测下列的攻击行为：

- Scanning Ports：这种攻击行为是通过扫描软件，扫描对方主机上所有的 Ports（1 至 65535），检测 Server 上每个 Port 的反应，以计算服务器中正在使用的服务（Service），然后进行攻击。
- IP Half：不断重复的连接到某台服务器主机，且没有建立实际的连接，这意味者入侵者（黑客）在检测开放的 Ports，并企图防止被主机系统记录（Log）。
- Land：入侵的方式是伪装（仿真）成某一台服务器主机，利用相同地址与 Port，发出一个 TCP 的 Request，以达到攻击的目的，这会造成一些 TCP 的程序代码死循环而死机。
- Ping of Death：入侵的方式是利用大量的 ICMP（一般使用的 Ping 工具）的 Request，发送到服务器主机，造成主机系统缓冲区（Buffer）溢出而死机。
- UDP Bomb：入侵的方式是通过传送一个非法的 UDP 包，此包的部分字段具有非法的值，可造成主机系统死机。
- DNS Hostname 溢出：当 DNS Server 恢复一个主机名称时，超过某个固定长度，如果应用程序没有检查主机名称的长度的话，可能会 Copy 主机名称返回内部缓冲区，这样允许了远程的入侵者（黑客）在服务器主机上执行破坏的命令。
- DNS Length 溢出：DNS 恢复的 IP 地址中，含有一个应为 4bytes 的长度字段，通过格式化 DNS 的恢复，给定一个较大的值，会造成一些应用程序内部缓冲区（Buffer）溢出。
- POP 缓冲区溢出：远程的攻击者，企图以溢出内部缓冲区（Buffer）方式，以得到访问 POP 服务器的 Root。

门禁管制（Outgoing Access Policy）

ISA Server 的门禁管制让内部与外部用户对于资源的访问具有非常安全的规范，所谓门

禁管制就是在 ISA Server 主机上，设置一些策略（Policy）与规则（Rule），在 ISA Server 企业版中，有两种等级的策略（Policy），分别说明如下：

- 阵列层的策略（Array-Level Policy）：在“阵列层”下建立站点规则（Site Rules）、内容规则（Content Rules）、通讯协议规则（Protocol Rules）、IP 包过滤（IP Packet Filter）、网站发布规则（Web Publishing）、其他服务器发布规则（Server Publishing）等，“阵列层的策略”决定内部网络的用户以什么方式连上 Internet，以及决定允许什么服务器主机可以传输数据。“阵列层的策略”适用在独立的主机或阵列主机上，即 Local 的策略，换句话说，在“阵列层的策略”里面设置的规范，不能控制到这群阵列外的主机以及分公司的网络策略，如果想控制远程网络（分公司）的一些网络访问策略，则必须使用“企业层的策略”。
- 企业层的策略（Enterprise-Level Policy）：“企业层的策略”适用任意阵列成员上，且能让阵列策略扩充，概念上，“企业层的策略”可以包括多个“阵列层的策略”，因为“阵列层的策略”可以分据多个不同地点，通过“企业层的策略”可以整合各地点的局域网里的访问策略。

总公司的 ISA Server 管理者可以制定宽松一点的“企业层的策略”，让分公司 Local 端的系统管理者做更细的“阵列层的策略”访问设计，发挥个体上的控制，是一个不错的方法，或者二者并存亦可。

不论哪一种层的 Policy，其内含的限制元素并没有顺序性，但 ISA Server 系统会对于“拒绝的规则”比“允许的规则”先处理，且“访问规则”会先使用存在于 ISA Server Cache 里的数据来响应，如果 Cache 里面没有需要的数据或数据已过期（TTL），就会抓防火墙外的真实数据来响应，且用户访问任何数据都要通过认证，只有在许可范围下的访问能被接受，不正当的访问行为将被阻挡，ISA Server 的门禁管制包括的元素如下：

- ✓ IP 地址。
- ✓ Active Directory 的用户、组。
- ✓ Internet 上的任何目的地 URLs。
- ✓ 各种通讯协议（Protocol Definition）。
- ✓ 计划时段（Schedule）。
- ✓ 带宽优先权（Bandwidth Rule）。

整体安全性（Security Integration）

ISA Serve 运行于 Windows Serve 2000 操作系统上，具有下列优异的安全性、性能、与管理：

- 网络地址转换（Network Address Translator ）：通过转译内部地址为外部地址，NAT 隐藏内部被管理的 IP 地址，让内部使用虚拟的 IP 地址，来降低 IP 地址的登录成本或解决 IP 地址不够用的问题，而对外则只转译少数 IP 地址，如此可减少内部系统受到攻击的风险。ISA Server 支持 Secure NAT Client，让内部用户只要是使用 TCP/IP 的 Protocol，不论是麦金塔（Macintosh）或 UNIX 均可兼容。
- 虚拟私有网络（VPN；Virtual Private Networking）：ISA Server 可以连接两个远程局域网络，然后打开一个私人安全的通讯信道，不论是直接对外连接或临时拨接，都

可以支持安全的网关对网关的通讯（PPTP），或是由单独一台使用计算机由远程对 ISA Server 打开 VPN 的安全通讯信道访问数据。

- 用户认证（User-Level Authentication）：ISA Server 支持所有 Windows Serve 2000 的 Active Directory 授权用户认证功能。
- 层次式策略管理（Hierarchical Policy）：ISA Server 企业版的设置文件与策略信息（Schema）集中储存在 Windows Serve 2000 的 Active Directory 里，所以企业管理者可轻易定义一至多个“企业层的策略”，并且套用到每个安装企业版的阵列服务器上。
- 网站过滤器（Web Filter）：ISA Server 网站过滤器可依据 Internet 服务器应用程序接口(ISAPI)建立，可以查看与控制流经防火墙的 HTTP 与 FTP 的数据流。
- 警告系统（Alert System）：ISA Server 的警告信息会写入 Windows Server 2000 的事件日志中，供管理者做排除或追踪处理等操作，同时管理者也可以自定警告信息来提醒自己（用 E-Mail）或其他管理者，立即处理系统的重要事件。

1-4-2 服务与发布的特色

所谓发布（Publish）指的是你要从内部网络提供什么服务（Service）给 Internet 的访问者，譬如：网站服务器、邮件服务器、新闻组服务器、FTP 服务器、数据库等，ISA Server 会保护在防火墙后的所有服务器与电子商务应用程序，免于外来的入侵与攻击，ISA Server 的服务与发布的特色介绍如下：

网站服务的发布（Web Publishing）：

你可以设置“网站发布”的规则（Rule），来决定是否要把 Internet 的 Request 送到 Local 端的网站服务器，一般来说，当一个在 Internet 上的访问者想阅读一个网页，这个 Request 实际上只被传送到 ISA Server，由 ISA Server 直接响应网页给访问者，访问者不会直接接触到真正的 Web Server（如图 1-2），如此可以加速网页访问的速度与提高网站的安全性。

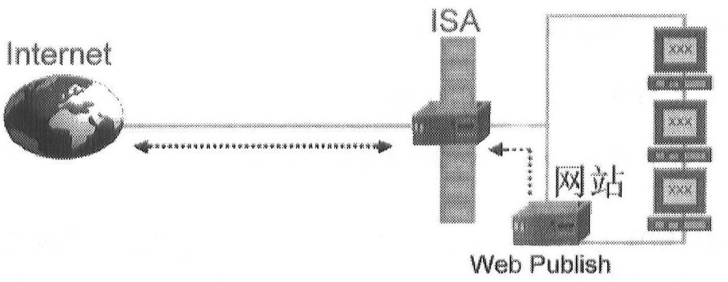


图 1-2 Internet 用户实际上只接触到 ISA Server

服务器服务的发布（Server Publishing）：

你可以设置“服务器发布”的规则（Rule），决定是否要把 Request 送到 Local 端相对应

的服务器。举例来说，如果你有安装邮件服务器，可以建立规则来允许邮件服务器被 Publishing 到 Internet，ISA Server 会拦截到邮件服务器的 Mail 信件，这样可以让 Internet 用户知道有个 E-mail Server，但你的邮件服务器却不会直接暴露到外界，维持了服务器的安全。ISA Server 可以检查 Mail 邮件里是否有被拒绝的内容、网域、附加文件、关键字等，譬如 I-Love-You 病毒，就可以通过此规则（Rule）排除掉，以免不知情的用户继续犯错。

带宽控制（Bandwidth Control）：

设置 Bandwidth 规则（Rule），决定哪一个用户、组、服务或整个局域网络在哪一个时段里，只能占用多少的带宽。

> **说明**
>
> 在阅读防火墙相关书籍或文件时，你应该常会看到一堆策略（Policy）与规则（Rule），一会儿 Policy、一会儿 Rule，两者应该如何区分？实际上，可以想成一个 Policy 是由一或多个 Rule 所组合而成的。

1-4-3 网络缓存的特色

启动“网络缓存”的功能，其目的除了有安全的利益外，最重要的应该是增加网络传输的速度，网络速度提升代表带宽、主机、应用程序的整体效益提升，如此一来，最起码就可为公司省下一笔可观的硬件升级费用。

ISA Server 高性能的缓存功能，包括由“内部网络”至“外部网络”，或“外部网络”至“内部网络”，双向都可以提高访问速度，就概念上及网络整体部署上，“网络缓存”分为以下四种（本书第 6 章将有详细说明）：

分布式缓存（Distributed Caching）：

ISA Server 企业版提供分布式（阵列式）的缓存，通过多台 ISA 服务器的串联的方式达到，可以提高系统负荷量、容错能力以及平衡性能。除此之外，分布式的缓存还可以由服务器阵列或服务器串联，或两者并用的方式架设。

分布式的缓存使用 CARP（Cache Array Routing Protocol）的技术，可以产生一种高效率无接缝式的缓存，使用上让多台缓存服务器形同一台，并且不会造成数据重复存放的情况（如图 1-3）。

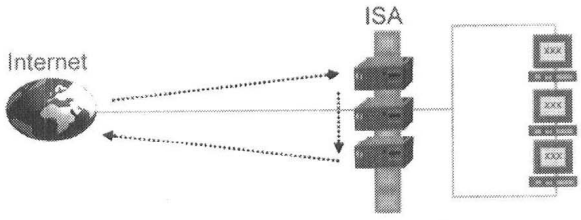


图 1-3 CARP 可以产生一种高效率无接缝式的缓存