



万水计算机核心技术精解系列

ISA Server 2000

企业组网实用大全



邓劲生 王斌 田艳芳 等编著



中国水利水电出版社
www.waterpub.com.cn

万水计算机核心技术精解系列

ISA Server 2000 企业组网实用大全

邓劲生 王斌 田艳芳 等编著

中国水利水电出版社

内 容 提 要

本书主要内容涵盖 ISA Server 2000 的安装准备、安装过程及疑难解决、从 Proxy Server 升级、规划并部署客户、策略和规则、身份验证、缓存和加速, 以及 Web Proxy 服务、保证内部网络的安全、支持媒体服务、发布服务、管理多台 ISA 服务器、ISA 服务器的集成服务、解决问题和报告工作、建立与外部客户的连接等章节, 全面深入地探讨如何利用 ISA Server 2000 来构建强大而安全的企业内部网络。在书的最后提供了一系列企业实施方案以及国外的一些成功范例, 相信对于 ISA Server 管理员大有裨益。

本书对于 ISA Server 网络管理员、技术支持工程师和系统开发工程师是全面的、权威的、不可或缺的参考书, 也适合于参加 MCSE 70-227 的考试人员学习。

图书在版编目 (CIP) 数据

ISA Server 2000 企业组网实用大全 / 邓劲生等编著. —北京: 中国水利水电出版社, 2002

(万水计算机核心技术精解系列)

ISBN 7-5084-1009-2

I. I… II. 邓… 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 015789 号

书 名	ISA Server 2000 企业组网实用大全
作 者	邓劲生 王斌 田艳芳 等编著
出版、发行	中国水利水电出版社 (北京市三里河路 6 号 100044) 网址: www.waterpub.com.cn E-mail: mchannel@public3.bta.net.cn (万水) sale@waterpub.com.cn
经 售	电话: (010) 68359286 (万水) 63202266 (总机) 68331835 (发行部) 全国各地新华书店
排 版	北京万水电子信息有限公司
印 刷	北京市天竺颖华印刷厂
规 格	787×1092 毫米 16 开本 24.75 印张 532 千字
版 次	2002 年 3 月第一版 2002 年 3 月北京第一次印刷
印 数	0001—5000 册
定 价	35.00 元

凡购买我社图书, 如有缺页、倒页、脱页的, 本社发行部负责调换

版权所有·侵权必究

前 言

Internet 访问是一种功能强大的工具。然而，就像其他的强大工具一样，Internet 访问也是一把双刃剑。它既能够显著地提高工作效率，又可能对工作效率产生重大的消极影响。对 Internet 危害性的正确看待，是产生积极影响的最佳实现方法。

Microsoft Internet Security and Acceleration (ISA) Server 2000 是与 Microsoft Windows 2000 紧密集成的可扩展企业防火墙与 Web 缓存服务器，它实现了基于策略的安全性、加速性及网络互连管理功能。这种最先进的防火墙产品直接面向管理需求而设计开发，可提供实质性网络保护功能，并能够对外来入侵实施检测和采取响应的对策。

用于 PC 机的 Windows 操作系统极大地改变了我们使用计算机的方式。Windows 使得计算机初学者也能够充分地利用 PC 机的威力，从而使得 PC 机融合在人们的日常生活中。而对于当前的 Internet 革命，Microsoft 推出 .NET 平台，希望像释放 PC 机的潜能一样来释放 Internet 的潜能，以改善那些使用 Internet 的人们生活。

ISA Server 的作用，就是保证那些使用 .NET 平台服务器的方案和服务的安全。ISA Server 2000 是 Proxy Server 2.0 的后继产品。ISA Server 通过提供企业级防火墙和高性能 Web 缓存服务器，远远超越了原有代理服务的范畴，从而能够满足当前 Internet 环境中最迫切的需求。名字的改变更为准确地反映出它对于向内和向外的连接都提供安全和加速服务。

本书的全部内容围绕安装、配置和管理 ISA Server 2000 企业版进行深入的探讨。每章的构造基本按照术语、原理、操作、实施和小结的模式进行，由浅入深逐步进行学习和运用。在每章中都有一个实际工程的实施过程，取材于企业中的真实场景，结合本章中所讨论的技术进行解决，从而更方便于读者将技术运用于企业的网络管理。

本书主要内容涵盖安装准备、安装过程及疑难解决、从 Proxy Server 升级、规划并部署客户、策略和规则、身份验证、缓存和加速，以及 Web Proxy 服务、保证内部网络的安全、支持媒体服务、发布服务、管理多台 ISA 服务器、ISA 服务器的集成服务、解决问题和报告工作、建立与外部客户的连接等章节，全面深入地探讨如何利用 ISA Server 2000 来构建强大而安全的企业内部网络。在书的最后提供了一系列企业实施方案以及国外的一些成功范例，相信对于 ISA Server 管理员大有裨益。

由于目前关于 ISA Server 的中文资料相对匮乏，我们的主要资料基本来源于 Internet 上的各种英文电子文档，比如 Microsoft 的知识库、MCSE 70-227 “安装、配置和管理 ISA Server 2000” 的原版教材、ISA Server 在线文档以及 Internet 上的讨论组等。在仔细地学习和消化这些资料之后，我们才开始着手本书的编写工作，以求能够保证准确性和完备性。

本书由邓劲生、王斌、田艳芳等人完成主要部分的编写工作，参加本书部分章节的编写

以及资料采集、文字录入、校对和排版的人员还有张晓明、虞万荣、刘锋、王涛、潘莉、宋辉、周斌、赵亮、王丰、任芳、叶少秋、张平运、雷易平、宁益民、金姜等。在此要特别感谢孙春亮老师，本书的顺利完成与他的辛勤劳动和热情支持是分不开的。

本书的主要编者都是大中型网络的管理员，他们目前从事内部网络的构建和维护工作，有着敬业的工作态度、丰富的工程经验和良好的协作习惯。但是由于全书内容覆盖面广且知识较新，而时间紧迫且编者水平有限，差错之处在所难免，恳请各位读者批评指正。

编者

2001年11月于砚瓦池

目 录

前言

第 1 章	ISA Server 2000 概述.....	1
1.1	Microsoft Proxy Server	2
1.1.1	不仅仅是一个升级	2
1.1.2	迁移的必要性	3
1.2	ISA Server 的特性	3
1.2.1	安全的 Internet 连接	3
1.2.2	快速的 Web 访问	4
1.2.3	简单统一的管理	5
1.2.4	可扩展的开放平台	6
1.3	.NET 平台	6
1.3.1	商业的革命	7
1.3.2	超越浏览模式和.com 模式	8
1.3.3	创建新一代 Internet	9
1.3.4	Microsoft .NET: 新一代产品和服务	11
1.4	Internet 连接	12
1.4.1	OSI 模型	12
1.4.2	TCP/IP 协议	13
1.4.3	统一资源定位 (URL)	13
1.5	端口和套接字	15
1.6	Internet 安全基础	16
1.6.1	何时它是防火墙	17
1.6.2	何时它是代理服务器	17
1.6.3	既然它们是如此不同, 那么为何不可以把它们区分开来	19
1.7	连接类型	19
1.7.1	数据报层连接	19
1.7.2	电路层连接	20
1.7.3	应用层连接	20
1.8	新功能和特性	20
1.8.1	安装	20

1.8.2 管理	21
1.9 作为防火墙的 ISA Server	22
1.10 作为代理的 ISA Server	23
可扩展性	23
1.11 实际工程	23
1.12 本章小结	25
第 2 章 ISA 服务器安装准备	26
2.1 硬件要求	26
2.1.1 防火墙要求	27
2.1.2 缓存要求	27
2.2 软件要求	28
2.3 纯安装还是从 Proxy Server 2.0 升级	29
2.4 ISA 服务器模式	29
2.5 ISA 服务器阵列	30
2.6 ISA 服务器客户支持	31
2.7 ISA 服务器安装前最后的系统准备	33
2.7.1 硬件配置	33
2.7.2 软件配置	34
2.8 实际工程	38
2.9 本章小结	43
第 3 章 安装 ISA Server 2000	45
3.1 ISA 服务器版本	45
硬件支持	46
3.2 安装之前	46
3.2.1 收集必要的信息	46
3.2.2 设置网络安装点	46
3.2.3 最近的软件升级	47
3.3 安装 ISA 服务器企业版	48
3.3.1 安装类型	48
3.3.2 独立服务器还是阵列	50
3.3.3 安装模式	53
3.3.4 为缓存设置磁盘空间	54
3.3.5 创建本地地址表 (LAT)	55
3.4 ISA 服务器的 Getting Started Wizard	57
3.5 脱机安装	57

3.5.1	理解每个区	58
3.5.2	运行脱机安装文件	60
3.6	安装期间创建或参加一个阵列	60
3.6.1	创建第一个阵列	60
3.6.2	加入一个阵列	61
3.6.3	将独立安装的企业版 ISA 服务器升级为一个阵列成员	61
3.7	ISA 服务器标准版的安装	62
3.8	删除 ISA 服务器	62
3.9	停止和启动 ISA Server 服务	62
3.10	实际工程	64
3.11	本章小结	68
第 4 章	从 Proxy Server 2.0 升级	69
4.1	为何要从 Proxy Server 2.0 迁移	69
4.1.1	10 倍于 Proxy Server 2.0 的运行速度	70
4.1.2	超强 Internet 访问控制	70
4.1.3	可伸缩的集中式管理	71
4.1.4	经过认证的企业防火墙	71
4.1.5	技术规范	72
4.2	升级的准备工作	73
4.2.1	协议配置	74
4.2.2	本地地址表	74
4.2.3	备份 Proxy Server 配置	74
4.3	NT 4 上的 Proxy Server	75
4.3.1	停止服务	75
4.3.2	执行第一次升级	77
4.3.3	升级到 ISA 服务器	77
4.4	从 Windows 2000 上的 Proxy Server 升级	79
4.5	升级 Proxy Server 阵列	80
4.6	配置从 Proxy Server 到 ISA 服务器的设置	80
4.6.1	不必重新配置的设置	80
4.6.2	需要重新配置的设置	81
4.7	进行管理更新	82
4.8	卸载 ISA 服务器	83
4.9	实际工程	83
4.10	本章小结	86

第 5 章 规划并部署客户	88
5.1 客户类型	88
5.1.1 想要做些什么	89
5.1.2 Web Proxy 客户	89
5.1.3 Firewall 客户	90
5.1.4 SecureNAT 客户	91
5.1.5 Socks	92
5.2 客户间的区别	93
客户联合	93
5.3 Web Proxy 客户设置	94
5.4 Firewall 客户设置	96
5.4.1 Firewall 客户安装期间发生更新	97
5.4.2 删除 Firewall 客户	97
5.5 配置 Firewall 客户文件	97
5.5.1 配置 msplat.txt 文件	98
5.5.2 配置 mspclnt.ini 文件	98
5.5.3 本地域表	100
5.6 SecureNAT 客户所需的设置	100
5.7 Socks 客户设置	101
自动检测设置	102
5.8 评估客户需求	103
5.8.1 客户连接需求	104
5.8.2 客户操作系统的差异	104
5.8.3 安全和设置要求	104
5.9 实际工程	104
5.10 本章小结	107
第 6 章 策略和规则	108
6.1 用 ISA 服务器控制访问	109
6.1.1 什么是策略	109
6.1.2 企业级策略和列级策略	109
6.1.3 需要策略吗	110
6.1.4 可以支持哪种策略	110
6.1.5 怎样使用规则	111
6.2 策略元素	111
6.2.1 协议定义	111

6.2.2	目标集	113
6.2.3	内容组	114
6.2.4	客户地址集	115
6.2.5	日程表	116
6.3	使用协议规则	118
6.3.1	创建协议规则	118
6.3.2	协议规则顺序	119
6.4	站点及内容规则	119
6.4.1	站点及内容规则怎样被应用	120
6.4.2	创建站点及内容规则	120
6.5	数据报过滤器	122
6.5.1	以前的数据报过滤器	123
6.5.2	现在的数据报过滤器	123
6.6	带宽规则	123
6.6.1	带宽优先级	124
6.6.2	创建并配置带宽规则	125
6.6.3	排序规则	126
6.6.4	禁用或删除规则	126
6.7	为网络规划策略	126
6.7.1	需要书面规划的策略	127
6.7.2	是想在企业级、阵列级还是在独立服务器上实现策略	127
6.7.3	想控制哪些设置	128
6.7.4	需要创建策略元素吗	128
6.7.5	创建并测试规则	128
6.8	为企业级策略创建企业级规则	128
6.9	备份和恢复策略设置	129
6.10	实际工程	130
6.11	本章小结	133
第 7 章	身份验证	134
7.1	为何使用身份验证	134
7.2	身份验证的类型	135
7.2.1	基本验证	135
7.2.2	摘要验证	136
7.2.3	集成的 Windows 验证	137
7.2.4	证书	138

7.3	身份验证的优缺点	139
7.4	设置身份验证	139
7.4.1	监听器	140
7.4.2	配置身份验证	140
7.4.3	编辑监听器来改变身份验证要求	142
7.5	传输身份验证请求	142
7.5.1	使用 Pass-through 身份验证	142
7.5.2	链式身份验证	143
7.6	结合规则和身份验证	143
7.7	实际工程	143
7.8	本章小结	146
第 8 章	缓存和加速	148
8.1	潜在的问题	148
8.2	缓存是什么	149
8.3	理解缓存过程	151
8.4	什么是 CARP	153
8.4.1	CARP 的优点	154
8.4.2	CARP 配置	155
8.5	预定缓存内容下载	156
8.6	缓存链	157
8.7	Web Proxy 路由	158
8.8	缓存过滤器	160
8.9	调整并监控缓存性能	160
8.9.1	调整 ISA 服务器	160
8.9.2	监控 ISA 服务器	161
8.10	实际工程	162
8.11	本章小结	173
第 9 章	理解 Web Proxy 服务	175
9.1	什么是 Web Proxy 服务	175
9.2	Web Proxy 服务使用的协议	176
9.2.1	HTTP 和 HTTP-S	176
9.2.2	FTP	177
9.2.3	Gopher	177
9.3	Web Proxy 服务的客户	177
9.3.1	CERN 兼容的 Web 浏览器	177

9.3.2	HTTP 重定向过滤器	177
9.4	Web Proxy 服务的工作方式	178
	Web Proxy 服务的扩展	179
9.5	通过 Web Proxy 服务访问安全网页	179
9.5.1	SSL 部件	179
9.5.2	使用证书创建一个身份	180
9.5.3	端口和协议	182
9.5.4	SSL 过程	182
9.6	ISA 服务器对安全网页的影响	182
9.6.1	SSL 隧道	183
9.6.2	SSL 桥接	183
9.6.3	SSL 和性能	184
9.7	配置 Web Proxy 服务	185
9.7.1	端口设置	185
9.7.2	监听器	185
9.7.3	SSL 监听器	186
9.7.4	配置 HTTP 重定向过滤器	186
9.7.5	连接设置	187
9.7.6	缓存设置	187
9.8	实际工程	188
9.9	本章小结	189
第 10 章	保证内部网络的安全	191
10.1	使用 Windows 2000 安全机制	191
10.1.1	ISA 服务器的 Security Configuration Wizard	192
10.1.2	使用 Security Configuration Wizard	193
10.2	ISA 服务器安全指标	194
10.3	非法入侵检查	195
10.4	配置非法入侵检查	196
10.5	配置警报器	197
10.6	实际工程	198
10.7	本章小结	205
第 11 章	支持媒体服务	207
11.1	什么是多媒体	207
11.2	什么是 H.323 Gatekeeper 服务	208
11.2.1	H.323 部件	209

11.2.2	与 H.323 兼容的应用	209
11.3	H.323 连接	210
11.3.1	H.323 Gatekeeper 规则和函数	211
11.3.2	不同类型的 RAS	211
11.4	H.323 部件及其设置	211
11.4.1	配置 H.323 协议过滤器	212
11.4.2	创建 H.323 协议规则	212
11.5	安装 H.323 Gatekeeper 服务	213
	添加 Gatekeeper 服务器	214
11.6	配置连接	214
11.6.1	Active Terminal	214
11.6.2	Active Calls	214
11.6.3	Call Routing	214
11.7	配置 H.323 Gatekeeper	218
11.8	向内连接的额外配置	219
11.9	流媒体过滤器	220
11.9.1	Windows 媒体服务器	221
11.9.2	媒体协议定义	221
11.10	实际工程	222
11.11	本章小结	225
第 12 章	发布服务	227
12.1	ISA 服务器是怎么保护内部服务器的呢	227
12.2	发布策略	228
12.2.1	配置 LAT	229
12.2.2	监听器	229
12.3	Web 发布规则	230
12.3.1	Web 发布规则的目标集	231
12.3.2	客户的类型	231
12.3.3	规则动作	231
12.3.4	安全预防措施	232
12.4	SSL 桥接	233
12.5	反向缓存	234
12.6	服务器发布规则	235
12.6.1	地址映射	235
12.6.2	协议设置	236

12.6.3	客户类型	236
12.6.4	服务器发布设置	236
12.7	设置一个邮件服务器	237
12.8	特殊的发布配置	237
12.9	发布一个邮件服务器	237
12.9.1	Mail Server Security Wizard	237
12.9.2	SMTP 过滤器	238
12.10	发布时使用数据报过滤器	242
12.11	配置发布规则	244
12.11.1	配置一个 Web 发布规则	244
12.11.2	配置一个服务器发布规则	245
12.12	内部服务器的设置	245
12.13	实际工程	245
12.14	本章小结	249
第 13 章	管理多台 ISA 服务器	250
13.1	什么是阵列	251
13.2	什么是链式结构	253
13.3	在阵列中安装 ISA 服务器	253
13.3.1	在阵列中安装第一台 ISA 服务器计算机	254
13.3.2	安装附加的阵列成员	255
13.3.3	将一个单独的服务器提升为一个阵列成员	255
13.3.4	更新策略设置	255
13.4	将 Proxy Server 2.0 提升为阵列	256
13.4.1	将 Proxy Server 2.0 提升为阵列时需要考虑的问题	256
13.4.2	迁移到阵列中	256
13.4.3	转换 Proxy Server 2.0 的配置	257
13.5	在 ISA 管理程序中创建和删除阵列	259
13.5.1	在 ISA 管理程序中创建阵列	259
13.5.2	从 ISA 管理程序中删除阵列	260
13.6	建立链式结构	260
13.7	备份和恢复企业版的配置	261
13.8	备份和恢复阵列的配置	262
13.9	使用企业策略和阵列策略	262
13.10	配置企业策略	262
13.10.1	指定默认的企业规则	263

13.10.2	更新企业策略的默认设置.....	263
13.10.3	将企业策略应用于选定的阵列中.....	263
13.11	配置 Web 发布策略.....	264
13.11.1	配置 ISA 服务器计算机.....	264
13.11.2	配置 DNS 服务器.....	264
13.11.3	本地网络上的 Web 发布方案.....	264
13.11.4	ISA 服务器计算机上的 Web 服务器.....	265
13.12	配置阵列策略.....	266
13.12.1	为阵列配置缓存.....	266
13.12.2	要求阵列进行数据包过滤.....	266
13.12.3	在阵列中允许发布规则.....	267
13.12.4	在 ISA 服务器上配置服务器指定的设置.....	267
13.13	将企业策略和阵列策略结合在一起.....	267
13.14	实际工程.....	268
13.15	本章小结.....	274
第 14 章	ISA 服务器的集成服务.....	276
14.1	为什么有些服务需要特殊的配置.....	276
14.2	在本地 ISA 服务器上集成服务.....	277
14.3	Exchange Server 和 ISA 服务器.....	277
Proxy Server 2.0 和 Exchange Server.....		277
14.4	邮件服务器安全向导.....	278
14.5	SMTP 过滤器.....	279
14.5.1	为 SMTP 过滤器配置 ISA 服务器和其他应用程序.....	280
14.5.2	配置 SMTP 过滤器属性页面.....	281
14.5.3	RPC 过滤器.....	284
14.5.4	DNS 的安装.....	284
14.6	在同一台机器上安装 Exchange Server 和 ISA 服务器.....	285
14.7	ISA 服务器和 NLB.....	285
14.7.1	安装 NLB.....	286
14.7.2	在 ISA 服务器上配置 NLB.....	287
14.7.3	NLB 的一个替代方案.....	288
14.8	ISA 服务器和活动目录的存储与复制.....	288
关于活动目录容器.....		289
14.9	ISA 服务器和终端服务.....	290
14.10	将 ISA 服务器和 Web 服务器集成.....	290

14.11	实际工程	291
14.12	本章小结	293
第 15 章	解决问题和报告工作	294
15.1	解决问题的指导方针	294
15.2	在 Windows 2000 中发现和解决问题的基本过程	295
	配置 IE5	299
15.3	解决问题的参考资源	300
15.4	在 ISA 服务器中发现和解决问题	301
15.4.1	解决与访问策略相关的问题	301
15.4.2	解决与授权有关的问题	302
15.4.3	解决与缓存有关的问题	303
15.4.4	解决与客户连接有关的问题	304
15.4.5	解决与拨号条目有关的问题	305
15.4.6	解决与记录有关的问题	306
15.4.7	解决与服务有关的问题	306
15.5	报告	307
15.5.1	创建报告	307
15.5.2	查看预定义的报告	309
15.5.3	配置报告	310
15.5.4	报告数据库	310
15.5.5	安排报告	311
15.5.6	信用	311
15.5.7	给一个报告工作指定用户信用	311
15.5.8	其他功能	312
15.6	实际工程	313
15.7	本章小结	321
第 16 章	建立与外部客户的连接	322
16.1	远程连接和客户	322
16.2	到达远处客户的连接	323
16.2.1	配置网络	323
16.2.2	配置 ISA 服务器	323
16.3	拨号网络与路由和远程访问服务	324
16.4	拨出到 Internet	325
16.5	拨号条目	325
16.5.1	配置拨号访问	326

16.5.2	设置活动拨号条目	328
16.5.3	跳过与 ISA 服务器的连接	328
16.6	虚拟专网 (VPN)	331
16.7	将 VPN 和 ISA 服务器集成	332
16.7.1	是本地还是远程	333
16.7.2	VPN 向导做的改变	334
16.7.3	是 PPTP 还是 L2TP	334
16.8	配置向导	334
16.8.1	本地 ISA VPN 向导	335
16.8.2	远程 ISA VPN 向导	337
16.8.3	从客户到 ISA 服务器的 VPN 向导	337
16.8.4	改变 VPN	338
16.9	带宽问题	339
16.9.1	识别带宽问题	340
16.9.2	设置有效带宽	342
16.10	实际工程	342
16.11	本章小结	345
第 17 章	企业实施方案	347
17.1	小型网络的方案	347
17.1.1	物理网络描述	347
17.1.2	问题	348
17.1.3	解决方法	348
17.1.4	安装新的 ISA 服务器的步骤	349
17.1.5	配置新的 ISA 服务器	349
17.1.6	配置客户	351
17.2	使用远程位置的网络	351
17.2.1	物理网络描述	352
17.2.2	问题	352
17.2.3	解决方案	353
17.2.4	配置三宿主的边界网络	353
17.2.5	配置 ISA 服务器	354
17.2.6	配置 SecureNAT 连接	356
17.3	更新需要增长设置的网络	356
17.3.1	物理网络描述	356
17.3.2	问题	357