

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP



HOW TO CHEAT AT CONFIGURING ISA Server 2004

Essential Knowledge on All Things ISA

- Written by the Industry's Most Trusted Source on ISA Server, Microsoft "Most Valuable Professionals" Tom and Deb Shinder
- Provides a Clear Migration Path from Earlier Versions of ISA Server
- Covers All New Features, Including Advanced Application-Layer Firewalls, VPNs, and Web Cache Solutions

Debra Littlejohn Shinder

Dr. Thomas W. Shinder

Martin Grasdal Technical Editor

Register for Free Membership to

s o l u t i o n s @ s y n g r e s s . c o m

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2004*, Brian Caswell and Jay Beale's *Snort 2.1 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy-to-search web page, providing you with the concise, easy-to-access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates and links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

HOW TO CHEAT AT Configuring ISA Server 2004

Dr. Thomas W. Shinder
Debra Littlejohn Shinder

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®,” “Ask the Author UPDATE®,” and “Hack Proofing®,” are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library”™, “Mission Critical™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	HJKVC458BH
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

How to Cheat at Configuring ISA Server 2004

Copyright © 2006 by Syngress Publishing, Inc. All rights reserved. Printed in Canada. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in Canada
1 2 3 4 5 6 7 8 9 0
ISBN: 1597490571

Publisher: Andrew Williams
Acquisitions Editor: Jaime Quigley
Technical Editor: Martin Grasdal
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editor: Edwina Lewis
Indexer: J. Edmund Rush

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.



Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Kathryn Barrett, John Chodacki, Rob Bullington, Aileen Berg, and Wendy Patterson.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.



Author Dedication

This book is dedicated to:

As always, our families: the kids (Kris and Kniki), the brothers (Rich and D), and our parents, including the ones who are no longer with us, as well as our extended families.

Our friends, many of whom are also our business colleagues—especially Stephen and Sean, Stu and Dan, Tony, John S. and Jody, and the many online communities to which we belong.

Our cats, Bobble and The Big Kitty, who walk on our keyboards, sleep on our desks and help to remind us that no matter how hectic life may be, there's always time to stop and smell the catnip.

As with all the others, we also dedicate this book to each other. Not many people are lucky enough to be able to work with their spouses, to spend twenty-four hours a day, most days, in each other's company, and to enjoy it this much. We are truly blessed.



About the Authors

Thomas W. Shinder, MD is an MCSE and has been awarded the Microsoft Most Valuable Professional (MVP) award for his work with ISA Server and is recognized in the firewall community as one of the foremost experts on ISA Server. Tom has consulted with major companies and organizations such as Microsoft Corp., Xerox, Lucent Technologies, FINA Oil, Hewlett-Packard, and the U.S. Department of Energy.

Tom practiced medicine in Oregon, Texas, and Arkansas before turning his growing fascination with computer technology into a new career shortly after marrying his wife, Debra Littlejohn Shinder, in the mid 90s. They co-own TACteam (Trainers, Authors, and Consultants), through which they teach technology topics and develop courseware, write books, articles, whitepapers and corporate product documentation and marketing materials, and assist small and large businesses in deploying technology solutions.

Tom co-authored, with Deb, the best selling *Configuring ISA Server 2000* (Syngress Publishing, ISBN: 1-928994-29-6), *Dr. Tom Shinder's ISA Server and Beyond* (Syngress, ISBN: 1-931836-66-3), and *Troubleshooting Windows 2000 TCP/IP* (Syngress, ISBN: 1-928994-11-3). He has contributed to several other books on subjects such as the Windows 2000 and Windows 2003 MCSE exams and has written hundreds of articles on Windows server products for a variety of electronic and print publications.

Tom is the “primary perpetrator” on ISAServer.org (www.isaserver.org), where he answers hundreds of questions per week on the discussion boards and is the leading content contributor.

Debra Littlejohn Shinder is an MCSE and has been awarded Microsoft's Most Valuable Professional (MVP) award in the area of Server Security. She is a former police officer and college level criminal justice instructor, which led her to her interest in computer security and computer crime. She has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook* (Syngress, ISBN: 1-931836-65-5), and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of the best selling *Configuring ISA Server 2000* (Syngress Publishing, ISBN: 1-928994-29-6), *Dr. Tom Shinder's ISA Server and Beyond* (Syngress, ISBN: 1-931836-66-3), and *Troubleshooting Windows 2000 TCP/IP* (Syngress, ISBN: 1-928994-11-3).

Deb is also a technical editor, developmental editor, and contributor to over 15 additional books on subjects such as the Windows 2000 and Windows 2003 MCSE exams, CompTIA Security+ exam and TruSecure's ICSA certification. She formerly edited the Brainbuzz A+ Hardware News and currently edits Sunbelt Software's *WXP News* (www.wxpnews.com) and the *Inside Windows Server Security* journal for Eli Journals. Her articles are regularly published on TechRepublic's TechProGuild site and Windowsecurity.com, and have appeared in print magazines such as Windows IT Pro Magazine (formerly Windows & .NET) and she has authored training material, corporate whitepapers, marketing material, and product documentation for Microsoft Corporation, DigitalThink, Sunbelt Software, CNET and other technology companies. Deb currently specializes in security issues and Microsoft products.

Deb and Tom live and work in the Dallas-Ft. Worth area and occasionally teach computer networking and security classes at Eastfield College.



Technical Editor

Martin Grasdal (MCSE+I, MCT, CNE,CNI, CTT, A+) An independent consultant with over 10 years experience in the computer industry, Martin has a wide range of networking and IT managerial experience. He has been an MCT since 1995 and an MCSE since 1996. His training and networking experience covers a number of products, including NetWare, Lotus Notes, Windows NT, Windows 2000, Windows 2003, Exchange Server, IIS, and ISA Server, among others. Martin currently works actively as a consultant, author and editor. His recent consulting experience includes contract work for Microsoft as a Technical Contributor to the MCP Program on projects related to server technologies. Martin lives in Edmonton, Alberta, Canada with his wife Cathy and their two sons.



From the Authors, Tom and Deb Shinder

ISA Server has been a big part of our lives for over five years. This is our fourth book about Microsoft's rapidly evolving firewall and caching solution, and it just keeps getting better. We're already looking forward to the release of the next version, code-named Wolverine, and looking ahead to the book(s) we'll write about it.

This book was a joint effort between the two of us, but it was also a team effort. There are dozens of people who contributed to the cause, without whom this book could not have been written:

We are deeply indebted to those on the ISA Server teams at Microsoft for involving us in the development, documentation and marketing of ISA. We especially want to thank those in Redmond, Dallas and Charlotte: Mike Nash, Steve Brown, Tony Bailey, Joseph Landes, Josue Fontanez, Marcus Schmidt, Risa Coleman, Mark Mortimer, Red Johnston, Dave Gardner, Joel Sloss, Julia Polk, Steve Riley, Zach Gutt, Mike Chan, Suzanne Kalberer, Kelly Mondloch, Alan Wood, Clint Denham, Ellen Prater, Scott Jiles, Sibylle Hauptert, Amy Logan, Ari Fruchter, Ronen Boazi, Barclay Neira, Ben Guterson, Colin Lyth, Eric Rosencrantz, Jan Shanahan, Jim Edwards, and Walter Boyd, and we also want to thank Joern Wittern and Ronald Beekelaar for all their help and support.

We also want to thank the ISA team in Israel: Avi Nathan, Adina Hagege, Keren Master, Ron Mondri, Itai Greenberg, Yossi Siles, Sigalit Bar, Nathan Bigman, Linda Lior, Neta Amit, Amit Finkelstein, Meir Shmouely, Nir Ben Zvi, Opher Dubrovsky, Oren Trutner, Yigal Edery, Ziv Mador, Raz Goren, Mooly Beeri, Nir Caliv, Ziv Caspi, Gergory Bershansky, Ariel Katz, Dan Bar-Lev, Max Uritsky, Ronen Barenboim, Nir Michalowicz and Uri Barash.

Thank you to the hardware vendors who gave us the opportunity to work with their ISA Server-based appliances: John Curtis, John Amaral, Mike Druar, Kevin Murphy, Erika Batten, Bonnie Anderson, and Mark Roden, of Network Engines, Abdul Azhan of RimApp, Marc Semadeni of Hewlett Packard, and Yong Thye Lin and Yong Ping Lin of Celestix.

We want to thank our technical editor, Martin Grasdahl, for his painstaking efforts to ensure that every procedure we outlined worked, that our descrip-

tions and instructions were accurate and complete, and that our text was understandable – even the parts that we wrote at the end of an 18 hour day when we were hanging onto consciousness and our sanity by virtue of sheer willpower and numerous cups of coffee. We also thank Edwina Lewis, our copy editor, who wrestled with the terminology, whose eagle eye spotted our typos, and who stayed sweet and cheerful even when we got a little grumpy.

We also want to thank Stephen Chetcuti and Sean Buttgieg of Isaserver.org (www.isaserver.org) and Windowsecurity.com (www.windowsecurity.com), who provided us with forums in which we were able to promote both ISA Server itself and this book, and through which we got to know other ISA Server fans all over the world.

Thank you, too, to John Sheesley at Tech Republic/TechProGuild (www.techproguild.com), which hosted our series of articles on ISA Server 2004, and Amy Eisenberg and Patricia Colby, at *Windows IT Pro Magazine* (formerly *Windows & .NET*), which featured a number of our ISA Server 2004 articles.

We want to recognize all the other ISA Server and Security MVPs whose ideas and help were invaluable in writing this book: Chris Gregory, Kai Wilke, Stefaan Pouseele, Jason Ballard, Bud Ratliff, Christian Groebner, Dieter Rauscher, Frédéric Esnouf, Jesper Hanno, Philippe Mathon, Phil Windell, Slav Pidgorny, Abraham Martínez Fernández, and Tim Mullen.

In addition, special thanks to those who've supported and maintained the MVP program: Jerry Bryant, Emily Freet, Melissa Travers, Janni Clark, and John Eddy.

In addition, we want to thank the participants in the ISA Server news-groups, mailing lists and message boards whose questions inspired many of the scenarios in this book, and others who contributed in various ways. In particular, we extend our gratitude to John Tolmachoff, Jeffrey Martin, Amy Babinchak, Steve Moffat, Greg Mulholland, Shawn Quillman, Joseph Kravitz, Tiago de Aviz, David Farinic, Aman Bedi, Bill Stewart, AWJ (Al), Susan Bradley, and many, many others. Thanks guys!

We also want to give special recognition to Jim Harrison. Jim works for Microsoft on the ISA Server QA team and maintains the exceptional Web site: www.isatools.org. Many of us would be lost without Jim's tools and his constant prodding to be better networkers and firewall admins than we are today.

All of the above were instrumental in the development and production of this book, but any errors or omissions lie solely on our heads. We tried to make the manuscript as accurate and mistake-free as possible, but perfection still eludes us. If we've left anyone out, please accept our sincerest apologies (these last days of finishing up the manuscript have been hectic, to say the least) and let us know so we can correct the mistake in the next edition of the book.

Lastly, we want to say a special thank you to the folks at Syngress Publishing who pushed us to do this book, who showed extraordinary patience and understanding as deadlines slipped, and who believed in us from the beginning, especially Andrew Williams, our publisher, and Jaime Quigley, our editor. This one was a little less painful than the one before, for all of us.

Contents

Chapter 1 ISA 2004 Network Concepts and Preparing the Network Infrastructure	1
How ISA Firewall's Define Networks and Network Relationships	2
ISA 2004 Multinetworking	6
The ISA Firewall's Default Networks	8
Local Host Network	8
Internal Network	10
External Network (default)	18
VPN Clients Network	19
Quarantined VPN Clients Network	19
Creating New Networks	20
Controlling Routing Behavior with Network Rules	22
The ISA 2004 Network Objects	24
Networks	25
Network Sets	25
Computers	27
Address Ranges	28
Subnets	29
Computer Sets	30
URL Sets	32
Domain Name Sets	33
Web Listeners	35
ISA Firewall Network Templates	35
Edge Firewall Template	36
Trihomed (3-Leg) or DMZ Template	38
Front Firewall Template	43
Back Firewall Template	47

Single Network Adapter or Unihomed Network Template	51
Dynamic Address Assignment on the ISA Firewall's External Interface	53
Dial-up Connection Support for ISA Firewalls, Including VPN Connections to the ISP	54
"Network Behind a Network" Scenarios (Advanced ISA Firewall Configuration)	58
Web Proxy Chaining as a Form of Network Routing	64
Firewall Chaining as a Form of Network Routing	71
Configuring the ISA Firewall as a DHCP Server	72
One More Time	73

Chapter 2 ISA 2004 Client Types and Automating Client Provisioning 75

Understanding ISA 2004 Client Types	76
Understanding the ISA 2004 SecureNAT Client	79
SecureNAT Client Limitations	81
SecureNAT Client Advantages	84
Name Resolution for SecureNAT Clients	86
Understanding the ISA 2004 Firewall Client	91
Allows Strong User/Group-Based Authentication for All Winsock Applications Using TCP and UDP Protocols	92
Allows User and Application Information to be Recorded in the ISA 2004 Firewall's Log Files	93
Provides Enhanced Support for Network Applications, Including Complex Protocols Requiring Secondary Connections	93
Provides "Proxy" DNS Support for Firewall Client Machines	93
The Network Routing Infrastructure Is Transparent to the Firewall Client	94
How the Firewall Client Works	97
Installing the Firewall Client Share	99
Installing the Firewall Client	100
Firewall Client Configuration	102

Client Side Firewall Client Settings	106
Firewall Client Configuration Files	107
Firewall Client Configuration at the ISA 2004 Firewall	111
ISA 2004 Web Proxy Client	112
Improved Performance for the Firewall Client and SecureNAT Client Configuration for Web Access . .	113
Ability to Use the Autoconfiguration Script to Bypass Sites (Direct Access)	113
Allows You to Provide Web Access (HTTP/HTTPS/FTP Download) Without Enabling Users Access to Other Protocols	114
Allows You to Enforce User/Group-based Access Controls Over Web Access	114
Allows you to Limit the Number of Outbound Web Proxy Client Connections	119
Supports Web Proxy Chaining, Which Can Further Speed Up Internet Access	120
ISA 2004 Multiple Client Type Configuration	122
Deciding on an ISA 2004 Client Type	124
Automating ISA 2004 Client Provisioning	125
Configuring DHCP Servers to Support Web Proxy and Firewall Client Autodiscovery	127
Install the DHCP Server	127
Create the DHCP scope	127
Create the DHCP 252 Scope Option and Add It to the Scope	129
Configure the Client as a DHCP Client	132
Configure the Client Browser to Use DHCP for Autodiscovery	133
Configure the ISA 2004 Firewall to Publish Autodiscovery Information	133
Making the Connection	134
Configuring DNS Servers to Support Web Proxy and Firewall Client Autodiscovery	134
Creating the wpad Entry in DNS	135

Configure the Client to Use the Fully-Qualified wpad Alias	137
Configure the Client Browser to Use Autodiscovery	140
Special Considerations for VPN Clients	140
Configure the ISA 2004 Firewall to Publish Autodiscovery Information	141
Making the Connection Using DNS for Autodiscovery	142
Automating Installation of the Firewall Client	142
Configuring Firewall Client and Web Proxy Client Configuration in the ISA Management Console	143
Group Policy Software Installation	147
Silent Installation Script	149
Systems Management Server (SMS)	150
One More Time	151

Chapter 3 Installing and Configuring the ISA Firewall Software 153

Pre-installation Tasks and Considerations	154
System Requirements	154
Configuring the Routing Table	156
DNS Server Placement	157
Configuring the ISA Firewall's Network Interfaces	159
Installation via a Terminal Services Administration Mode Session	163
Performing a Clean Installation on a Multihomed Machine	163
Default Post-installation ISA Firewall Configuration	169
The Post-installation System Policy	171
Performing a Single NIC Installation (Unihomed ISA Firewall)	182
Quick Start Configuration for ISA Firewalls	184
Configuring the ISA Firewall's Network Interfaces	186
IP Address and DNS Server Assignment	186
Network Interface Order	188
Installing and Configuring a DNS Server on the ISA Server Firewall	189
Installing the DNS Service	189

Configuring the DNS Service on the ISA Firewall . . .	190
Configuring the DNS Service on the Internal Network DNS Server	193
Installing and Configuring a DHCP Server on the ISA Server Firewall	195
Installing the DHCP Service	195
Configuring the DHCP Service	196
Installing and Configuring the ISA Server 2004 Software	198
Configuring the ISA Firewall	200
Configuring the Internal Network Computers	208
Configuring Internal Clients as DHCP Clients	209
Hardening the Base ISA Firewall	
Configuration and Operating System	211
ISA Firewall Service Dependencies	212
Service Requirements for Common Tasks Performed on the ISA Firewall	214
Client Roles for the ISA Firewall	217
ISA Firewall Administrative Roles and Permissions	219
Lockdown Mode	221
Lockdown Mode Functionality	221
Connection Limits	222
DHCP Spoof Attack Prevention	224
One More Time	226
Chapter 4 Creating and Using ISA 2004 Firewall Access Policy	227
Introduction	228
ISA Firewall Access Rule Elements	230
Protocols	230
User Sets	231
Content Types	232
Schedules	238
Network Objects	239
Configuring Access Rules for Outbound Access through the ISA Firewall	239
The Rule Action Page	239

The Protocols Page	240
The Access Rule Sources Page	242
The Access Rule Destinations Page	242
The User Sets Page	243
Access Rule Properties	244
The General Tab	244
The Action Tab	244
The Protocols Tab	245
The From Tab	246
The To Tab	247
The Users Tab	248
The Schedule Tab	249
The Content Types Tab	249
The Access Rule Context Menu Options	250
Configuring RPC Policy	251
Configuring FTP Policy	252
Configuring HTTP Policy	252
Ordering and Organizing Access Rules	252
How to Block Logging for Selected Protocols	253
Disabling Automatic Web Proxy	
Connections for SecureNAT Clients	254
Using Scripts to Populate Domain Name Sets	255
Using the Import Scripts	258
Extending the SSL Tunnel Port Range	
for Web Access to Alternate SSL Ports	262
Avoiding Looping Back through the	
ISA Firewall for Internal Resources	264
Anonymous Requests Appear in	
Log File Even When Authentication	
is Enforced For Web (HTTP Connections)	266
Blocking MSN Messenger using an Access Rule	266
Allowing Outbound Access to	
MSN Messenger via Web Proxy	269
Changes to ISA Firewall Policy	
Only Affects New Connections	270

Allowing Intradomain Communications through the ISA Firewall	271
One More Time	279

Chapter 5 Publishing Network Services with ISA 2004 Firewalls 281

Overview of Web Publishing and Server Publishing	282
Web Publishing Rules	282
Provide Proxied Access to Web Sites Protected by the ISA Firewall	283
Perform Deep Application-Layer Inspection of Connections Made to Published Web Sites	283
Path Redirection	284
Pre-authentication of Connections Made to Published Web Sites	284
Reverse Caching of Published Web Sites	285
Ability to Publish Multiple Web Sites with a Single IP Address	285
Ability to Rewrite URLs Returned by the Published Web Site using the ISA Firewall's Link Translator . . .	286
Support for Forwarding Either the ISA Firewall's IP Address, or the Original Web Client's IP Address to the Web Site	286
Support for SecurID Authentication	287
Support for RADIUS Authentication	287
Ability to Schedule when Connections are Allowed to Published Web Sites	287
Port and Protocol Redirection	287
Server Publishing Rules	288
Server Publishing Rules are a Form of Reverse NAT or "Port Mapping" and do not Proxy the Connection	288
Almost All IP Level and TCP/UDP Protocols Can be Published using Server Publishing Rules . . .	289
Server Publishing Rules do not Support Authentication	289

Application-Layer Filtering can be Applied To a Defined Subset of Server Published Protocols	289
Configuring Port Overrides to Customize the Listening Ports and the Port Redirection	290
You can use IP Address Controls Over who can Access Published Resources	290
External Client Source IP Address can be Preserved or Replaced with the ISA Firewall's IP Address	290
Apply Schedules Limiting when the Published Server can be Accessed via the Server Publishing Rule	290
Support for Port Redirection or PAT (Port Address Translation)	290
Creating and Configuring Non-SSL Web Publishing Rules	291
The Select Rule Action Page	291
The Define Website to Publish Page	292
The Public Name Details Page	294
The Select Web Listener Page and Creating an HTTP Web Listener	295
The User Sets Page	303
The Web Publishing Rule Properties Dialog Box	304
The General Tab	304
Action	305
From	305
To	306
Traffic	307
Listener	308
Public Name	309
Paths	309
Bridging	313
Users	314
Schedule	315
Link Translation	316
Creating and Configuring SSL Web Publishing Rules	317
SSL Bridging	317
SSL "Tunneling" versus SSL "Bridging"	318

What About SSL-to-HTTP Bridging?	319
Enterprise and Standalone Certificate Authorities . . .	319
SSL-to-SSL Bridging and Web Site Certificate Configuration	321
Importing Web Site Certificates into the ISA Firewall's Machine Certificate Store	322
Requesting a User Certificate for the ISA Firewall to Present to SSL Web Sites	324
Creating an SSL Web Publishing Rule	326
The Publishing Mode Page	327
The Select Rule Action page	327
The Bridging Mode Page	328
The Define Website to Publish Page	329
The Public Name Details Page	330
The Select Web Listener Page	332
The User Sets Page	335
The SSL Web Publishing Rule Properties Dialog Box	335
Creating Server Publishing Rules	335
The Server Publishing Rule Properties Dialog Box	340
Server Publishing HTTP Sites	344
Creating Mail Server Publishing Rules	346
The Web Client Access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync Option	347
The Client Access: RPC, IMAP, POP3, SMTP Option	349
One More Time	352

Chapter 6 Creating Remote Access and Site-to-Site VPNs with ISA Firewalls 353

Overview of ISA Firewall VPN Networking	354
Firewall Policy Applied to VPN Client Connections . . .	355
Firewall Policy Applied to VPN Site-to-Site Connections	356
VPN Quarantine	357
User Mapping of VPN Clients	358
SecureNAT Client Support for VPN Connections . . .	358

Site-to-Site VPN Using Tunnel Mode IPSec	360
Publishing PPTP VPN Servers	360
Pre-shared Key Support for IPSec VPN Connections	361
Advanced Name Server Assignment for VPN Clients	362
Monitoring of VPN Client Connections	362
Creating a Remote Access PPTP VPN Server	363
Enable the VPN Server	364
Create an Access Rule Allowing	
VPN Clients Access to Allowed Resources	371
Enable Dial-in Access	373
Test the PPTP VPN Connection	375
Creating a Remote Access L2TP/IPSec Server	376
Issue Certificates to the ISA Firewall and VPN Clients	377
Test the L2TP/IPSec VPN Connection	382
Monitor VPN Clients	383
Using a Pre-shared Key for VPN	
Client Remote Access Connections	383
Creating a PPTP Site-to-Site VPN	385
Create the Remote Site Network at the Main Office	388
Create the Network Rule at the Main Office	390
Create the Access Rules at the Main Office	391
Create the VPN Gateway Dial-in	
Account at the Main Office	393
Create the Remote Site Network at the Branch Office	395
Create the Network Rule at the Branch Office	396
Create the Access Rules at the Branch Office	397
Create the VPN Gateway Dial-in	
Account at the Branch Office	398
Activate the Site-to-Site Links	399
Creating an L2TP/IPSec Site-to-Site VPN	400
Enable the System Policy Rule	
on the Main Office Firewall	
to Access the Enterprise CA	401
Request and Install a Web Site	
Certificate for the Main Office Firewall	402

Configure the Main Office ISA	
Firewall to Use L2TP/IPSec for the Site-to-Site Link . . .	405
Enable the System Policy Rule on the Branch	
Office Firewall to Access the Enterprise CA	405
Request and Install a Web Site	
Certificate for the Branch Office Firewall	406
Configure the Main Office ISA Firewall	
to Use L2TP/IPSec for the Site-to-Site Link	407
Activate the L2TP/IPSec	
Site-to-Site VPN Connection	408
Configuring Pre-shared Keys for	
Site-to-Site L2TP/IPSec VPN Links	409
IPSec Tunnel Mode Site-to-Site VPNs	
with Downlevel VPN Gateways	409
Using RADIUS for VPN	
Authentication and Remote Access Policy	410
Configure the Internet	
Authentication Services (RADIUS) Server	411
Create a VPN Clients Remote Access Policy	412
Remote Access Permissions	
and Domain Functional Level	414
Changing the User Account Dial-in Permissions	415
Changing the Domain Functional Level	416
Controlling Remote Access Permission	
via Remote Access Policy	417
Enable the VPN Server on the ISA	
Firewall and Configure RADIUS Support	418
Create an Access Rule Allowing	
VPN Clients Access to Approved Resources	420
Make the Connection from a PPTP VPN Client	422
Using EAP User Certificate	
Authentication for Remote Access VPNs	423
Configuring the ISA Firewall	
Software to Support EAP Authentication	424
Enabling User Mapping for	
EAP Authenticated Users	425

Issuing a User Certificate to the Remote Access VPN Client Machine	426
Supporting Outbound VPN Connections through the ISA Firewall	428
Installing and Configuring the DHCP Server and DHCP Relay Agent on the ISA Firewall	431
One More Time	434

Chapter 7 ISA 2004 Stateful Inspection and Application Layer Filtering 435

Introduction	436
Application Filters	437
The SMTP Filter and Message Screener	437
Installing the SMTP Message Screener on a Dedicated SMTP Relay	438
The DNS Filter	449
The POP Intrusion Detection Filter	450
The SOCKS V4 Filter	450
The FTP Access Filter	452
The H.323 Filter	452
The MMS Filter	453
The PNM Filter	453
The PPTP Filter	453
The RPC Filter	453
The RTSP Filter	453
Web Filters	454
The HTTP Security Filter (HTTP Filter)	454
Overview of HTTP Security Filter Settings	455
HTTP Security Filter Logging	465
Exporting and Importing HTTP Security Filter Settings	466
Investigating HTTP Headers for Potentially Dangerous Applications	468
Example HTTP Security Filter Policies	471
Commonly Blocked Headers and Application Signatures	475
The ISA Server Link Translator	476

Determining Custom Dictionary Entries	479
Configuring Custom Link	
Translation Dictionary Entries	480
The Web Proxy Filter	481
The OWA Forms-based Authentication Filter	482
The RADIUS Authentication Filter	482
IP Filtering and Intrusion Detection/Intrusion Prevention	483
Common Attacks Detection and Prevention	483
DNS Attacks Detection and Prevention	485
IP Options and IP Fragment Filtering	485
Source Routing Attack	486
One More Time	486

Chapter 8 Accelerating Web Performance with ISA 2004 Caching Capabilities 487

Understanding Caching Concepts	488
Web Caching Types	488
Forward Caching	488
Reverse Caching	489
Web Caching Architectures	490
Web Caching Protocols	492
Understanding ISA Server 2004's Web	
Caching Capabilities	493
Using the Caching Feature	494
Understanding Cache Rules	495
Using Cache Rules to Specify	
Content Types That Can Be Cached	495
Using Cache Rules to Specify How	
Objects are Retrieved and Served from Cache	496
Understanding the Content Download Feature	497
Configuring ISA Server 2004 as a Caching Server	498
Enabling and Configuring Caching	499
How to Enable Caching in Standard Edition	499
How to Disable Caching in Standard Edition	500
How to Configure Caching Properties	500
Configuring Which Content to Cache	500

Configuring the Maximum Size of Objects in the Cache	501
Configuring Whether Expired Objects Should be Returned from Cache	502
Allocating a Percentage of Memory to Caching	502
Creating Cache Rules	503
How to Create a Cache Rule	503
How to Modify an Existing Cache Rule	507
How to Disable or Delete a Cache Rule	508
How to Change the Order of Cache Rules	508
How to Copy a Cache Rule	508
How to Export and Import Cache Rules	509
Configuring Content Downloads	511
How to Ensure a Content Download Job Can Run	511
How to Create and Configure Scheduled Content Download Jobs	515
How to Make Changes to an Existing Content Download Job	517
How to Disable or Delete Content Download Jobs	518
How to Export and Import Content Download Job Configurations	518
How to Run a Content Download Job Immediately	519
One More Time	520

Chapter 9 Using ISA Server 2004's Monitoring, Logging, and Reporting Tools 521

Introduction	522
Exploring the ISA Server 2004 Dashboard	523
Dashboard Sections	524
Dashboard Connectivity Section	524
Dashboard Services Section	526
Dashboard Reports Section	526
Dashboard Alerts Section	527
Dashboard Sessions Section	528
Dashboard System Performance Section	528
Configuring and Customizing the Dashboard	530
Creating and Configuring ISA Server 2004 Alerts	530

Alert-triggering Events	530
Viewing the Predefined Alerts	532
Creating a New Alert	532
Modifying Alerts	537
Viewing Triggered Alerts	537
Monitoring ISA Server 2004	
Connectivity, Sessions, and Services	539
Configuring and Monitoring Connectivity	539
Creating Connectivity Verifiers	540
Monitoring Connectivity	543
Monitoring Sessions	545
Viewing, Stopping and Pausing	
Monitoring of Sessions	546
Monitoring Specific Sessions Using	
Filter Definitions	547
Disconnecting Sessions	549
Exporting and Importing Filter Definitions	550
Monitoring Services	550
Working with ISA Server 2004 Logs and Reports	551
Understanding ISA Server 2004 Logs	551
Log Types	551
How to Configure Logging	553
How to Use the Log Viewer	556
How to Filter the Log Information	557
Saving Log Viewer Data to a File	559
Exporting and Importing Filter Definitions	560
Generating, Viewing, and Publishing	
Reports with ISA Server 2004	560
How to Generate a One-time Report	561
How to Configure an Automated Report Job	563
Other Report Tasks	564
How to View Reports	566
Publishing Reports	566
Using ISA Server 2004's Performance Monitor	567
Index.	571

Chapter 1

ISA 2004 Network Concepts and Preparing the Network Infrastructure

Topics in this chapter:

- How ISA Firewalls Define Networks and Network Relationships
- Web Proxy Chaining as a Form of Network Routing
- Firewall Chaining as a Form of Network Routing
- Configuring the ISA Firewall as a DHCP Server

In this chapter, we will discuss a disparate group of issues that relate to the ISA firewall's Networking capabilities. We'll start with a detailed discussion of how we see the ISA firewall and its proper place on corporate networks. Then, we'll cover the network layout we use for all the scenarios discussed in this book. Included in this discussion will be a detailed description on how you can configure VMware to replicate the configurations in this book.

Next, we'll dig into the deep details on how the ISA firewall "sees" Networks, and how you configure the firewall to communicate on local and non-local networks. We'll also discuss some topics that don't fit neatly into any category, but seem to fit best into this "Network Concepts" chapter. We'll finish up with a discussion of the supporting Network Services that you will need to consider when setting up an ISA firewall. This is a critical discussion because the ISA firewall benefits from the services and support of a wide variety of network services.

In some of the discussions in this chapter, we'll cover concepts and procedures that will be discussed in much more detail in other chapters of this book. We understand if you find yourself frustrated with some terms or concepts in this chapter that haven't yet been defined. Be patient and look up those terms or concepts in other chapters in this book. You're also welcome to post a question on the www.isaserver.org message boards. Just write **BOOK** at the beginning of the title in your post and reference that page number of the book that you're having problems with, then send me an e-mail message at tshinder@isaserver.org with the link to your post.

How ISA Firewall's Define Networks and Network Relationships

One of the primary limitations of the ISA Server 2000 firewall was its simplistic view of the network. The ISA Server 2000 firewall recognized only two types of networks: trusted and untrusted. Trusted networks were included in the ISA Server 2000 firewall's Local Address Table (LAT). Any network that wasn't in the LAT was considered untrusted. ISA firewall policy was applied to all communications between LAT and non-LAT hosts.

Communications between LAT hosts were routed through the ISA Server 2000 firewall without being subjected to the ISA Server 2000 firewall's stateful filtering and application-layer inspection mechanisms.

This was problematic for ISA Server 2000 firewall administrators who wanted to create DMZ segments that were directly connected to the ISA Server 2000 firewall. For example, an ISA Server 2000 firewall might be configured with three network interfaces. This configuration could include an internal interface connecting to the internal network, a DMZ interface connected to a public access DMZ segment, and an external interface, which connects the firewall to the Internet.

In ISA Server 2000, this trihomed DMZ configuration highlights most of the limitations of the ISA Server 2000 networking model.

- All communications between LAT and non-NAT hosts had to be NATed. This meant that all connections between the internal network and the Internet, and the internal network and the DMZ segment, were NATed.
- The ISA Server 2000 firewall did not apply stateful application-layer inspection to connections between Internet hosts and machines on the DMZ segment. These

connections were routed by the ISA Server 2000 firewall from the Internet to the DMZ segment and only stateful filtering was done on the connections, similar to what you see with a typical hardware firewall.

- Communications between DMZ hosts and hosts on the internal network had to be accomplished via Server and Web Publishing Rules because the Internal network saw the DMZ segment as just another untrusted network.
- Outbound connections from the internal network to the DMZ segment were subject to the same Access Policy as those between the internal network and the Internet. For example, if you allowed outbound FTP access from the Internal network, FTP access was allowed to *all* non-LAT networks. If you allowed outbound access to a particular protocol, internal network users had access to that protocol at *all* sites.
- With the ISA Server 2000 firewall, it was possible to substitute private addresses for public address in the DMZ segment. However, the ISA Server 2000 firewall did not recognize this segment as a DMZ, and the DMZ segment had to be placed on the LAT. Because the ISA Server 2000 firewall only applied firewall policy on communications between LAT and non-LAT hosts, no firewall filtering was done between the internal network and the private address DMZ segment. While you could use RRAS packet filters to create a “poor man’s” DMZ segment, the RRAS packet filters provided even less flexibility and security than a hardware firewall’s stateful packet-filtering mechanisms.

Microsoft recognized these limitations in the ISA Server 2000 firewall and corrected them. The ISA firewall no longer uses the LAT. The LAT is no longer required because the ISA firewall does not implicitly trust any network. In ISA Server 2000, the LAT determined which networks were trusted and which were not. Because the networking model of the new ISA firewall does not trust any networks by default, the LAT is not part of the ISA firewall’s configuration. All communications moving through the ISA firewall are subject to the ISA firewall’s stateful filtering and stateful application-layer inspection mechanisms.

Another major improvement to the ISA firewall’s networking model is that you now have control over the routing relationship between the any two networks. For example, if you wanted to replicate the trihomed DMZ setup where you have an external interface, internal interface and DMZ interface, you can use public or private addresses on the DMZ segment and create a route or NAT relationship between the internal network and the DMZ segment. You can even choose between a route or NAT relationship between the internal network and the Internet. This is especially helpful if you have public addresses on your internal network and you want to continue using them without NATing outbound connections to the Internet.

Table 1.1 shows what’s new and improved in the ISA firewall’s networking model versus the ISA Server 2000.

Table 1.1 New and Improved Features in the ISA Firewall's Networking Model

Feature	Description
All Access Rules include a source and destination network element	Access Rules control what communications move through the firewall. Two of the key components of an Access Rule are the source of the connection request and the destination requested. That allows you fine-tuned control over protocol access through the firewall. You can allow users IRC access, but only when the request comes from a specific internal network and the destination is another network on the corporate LAN. IRC requests to any other network, including the Internet, are denied.
All communications moving through the ISA firewall are subjected to stateful filtering and stateful application-layer inspection	All connections made through the ISA firewall are subjected to the ISA firewall's Access Policies. There are no trusted networks in the ISA 2004 networking scheme. While you can choose to route all communications from one network to another via an Access Rule, there is never a requirement to do so.
Communications between any two networks can be routed or NATed	You can choose to route or to NAT connections between any two networks. You can choose a NAT relationship if you need to hide addresses on one network from another network, or you can route packets from one network to another network if you need to use protocols that do not function across NATed connections. The ability to choose the routing relationship between any two networks provides a great deal more flexibility than the ISA Server 2000 method of always NATing between LAT and non-NAT networking and always routing between LAT networks.
Firewall client and Web Proxy client configurations can be created on a per network basis	You can create multiple Internal networks and control access between these internal networks using Access Rules. Each network can have its own customized Web Proxy and Firewall client configuration and support. You may want one network to have Web Proxy client access but not Firewall client access, while at the same time, you want another internal network to have Firewall client access but not Web Proxy client access. You couldn't do this with the ISA Server 2000 firewall.
The ISA firewall is defined as a unique network	One of the most important jobs for a firewall is the ability to protect itself. One major limitation to the ISA Server 2000 firewall is that the packet-filtering mechanism only applied to non-LAT interfaces. This left LAT interfaces completely open to connections from any LAT host. The ISA firewall defines all its own interfaces as part of a <i>Local Host</i> network, and explicit Access Rules must be created to allow connections to <i>any</i> interface on the ISA firewall.

Continued