SYNGRESS®

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

solutions@syngress.com

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.

SYNGRESS®

SYNGRESS®

How to Cheat at Configuring ISA Server 2004

Dr. Thomas W. Shinder
Debra Littlejohn Shinder

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

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 Haupert, 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 Wettern 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 Michalowitz 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 Grasdal, 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 newsgroups, 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

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 firewalls 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 fined-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 *Local Host* network, and explicit Access Rules must be created to allow connections to *any* interface on the ISA firewall.

Continued