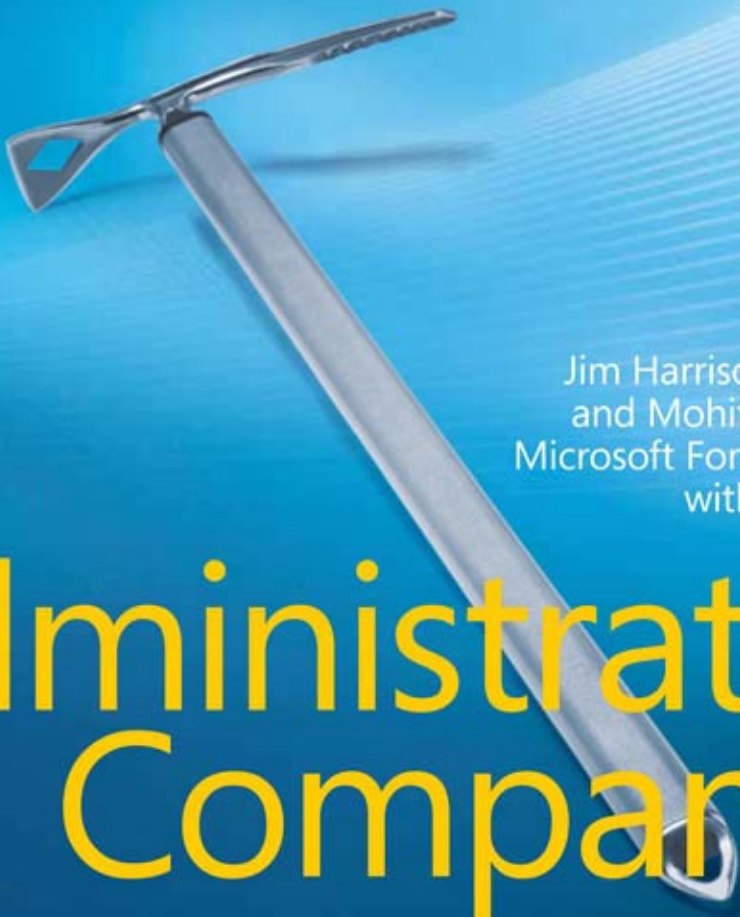


Microsoft®
**Forefront® Threat
Management
Gateway (TMG)**

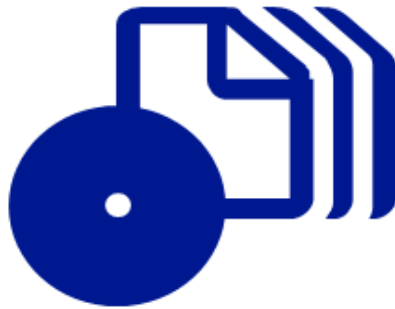


Jim Harrison, Yuri Diogenes,
and Mohit Saxena from the
Microsoft Forefront TMG Team
with Dr. Tom Shinder

**Administrator's
Companion**



How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to <http://aka.ms/626386/files>, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2010 by Jim Harrison, Yuri Diogenes, and Mohit Saxena

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2009943415

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 WCT 5 4 3 2 1 0

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Microsoft, Microsoft Press, Access, Active Directory, ActiveX, Forefront, Internet Explorer, Jscript, MS, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Martin DelRe

Developmental Editor: Karen Szall

Project Editor: Carol Vu

Editorial Production: Christian Holdener, S4Carlisle Publishing Services

Technical Reviewer: Dr. Tom Shinder; Technical Review services provided by Content Master,
a member of CM Group, Ltd.

Cover: Tom Draper Design

Body Part No. X16-38617

Contents at a Glance

Introduction

xxxi

PART I	A NEW ERA FOR THE MICROSOFT FIREWALL	
CHAPTER 1	What's New in TMG	3
CHAPTER 2	What Are the Differences Between TMG and UAG?	21
PART II	PLANNING FOR TMG	
CHAPTER 3	System Requirements	35
CHAPTER 4	Analyzing Network Requirements	47
CHAPTER 5	Choosing the Right Network Topology	65
CHAPTER 6	Migrating to TMG	87
CHAPTER 7	Choosing a TMG Client Type	107
PART III	IMPLEMENTING A TMG DEPLOYMENT	
CHAPTER 8	Installing TMG	141
CHAPTER 9	Troubleshooting TMG Setup	169
CHAPTER 10	Exploring the TMG Console	185
PART IV	TMG AS YOUR FIREWALL	
CHAPTER 11	Configuring TMG Networks	209
CHAPTER 12	Understanding Access Rules	241
CHAPTER 13	Configuring Load-Balancing Capabilities	263
CHAPTER 14	Network Inspection System	307
PART V	TMG AS YOUR CACHING PROXY	
CHAPTER 15	Web Proxy Auto Discovery for TMG	345
CHAPTER 16	Caching Concepts and Configuration	387

PART VI	TMG CLIENT PROTECTION	
CHAPTER 17	Malware Inspection	427
CHAPTER 18	URL Filtering	465
CHAPTER 19	Enhancing E-Mail Protection	487
CHAPTER 20	HTTP and HTTPS Inspection	529
PART VII	TMG PUBLISHING SCENARIOS	
CHAPTER 21	Understanding Publishing Concepts	573
CHAPTER 22	Publishing Servers	599
CHAPTER 23	Publishing Microsoft Office SharePoint Server	661
CHAPTER 24	Publishing Exchange Server	697
PART VIII	REMOTE ACCESS	
CHAPTER 25	Understanding Remote Access	733
CHAPTER 26	Implementing Dial-in Client VPN	747
CHAPTER 27	Implementing Site-to-Site VPN	773
PART IX	LOGGING AND REPORTING	
CHAPTER 28	Logging	797
CHAPTER 29	Enhanced NAT	817
CHAPTER 30	Scripting TMG	829
PART X	TROUBLESHOOTING	
CHAPTER 31	Mastering the Art of Troubleshooting	851
CHAPTER 32	Exploring HTTP Protocol	869
CHAPTER 33	Using Network Monitor 3 for Troubleshooting TMG	891
	<i>Appendix A: From Proxy to TMG</i>	911
	<i>Appendix B: TMG Performance Counters</i>	937
	<i>Appendix C: Windows Internet Libraries</i>	967
	<i>Appendix D: WPAD Script CARP Operation</i>	973
	<i>Index</i>	981

Contents

Introduction

xxxi

PART I A NEW ERA FOR THE MICROSOFT FIREWALL

Chapter 1	What's New in TMG	3
	Introducing TMG	3
	New Feature Comparisons	4
	Management Console	5
	Deployment	5
	Traffic Filtering	6
	Beyond the Firewall	8
	Integration: The Security Challenge	8
	Types of Firewalls	9
	Where TMG Fits In	10
	What's New?	11
	Windows Server 2008, Windows Server 2008 R2, and Native 64-Bit Support	12
	Web Antivirus and Anti-Malware Support	12
	Enhanced User Interface, Management, and Reporting	14
	URL Filtering	16
	HTTPS Inspection	16
	E-Mail Anti-Malware and Anti-Spam Support	16
	Network Intrusion Prevention	17

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:
microsoft.com/learning/booksurvey

	The Session Initiation Protocol (SIP) Filter	18
	TFTP Filter	18
	Network Functionality Enhancements	18
	Feature Comparison Summary	19
	Summary.....	20
Chapter 2	What Are the Differences Between TMG and UAG?	21
	Enabling Anywhere Access	22
	Understanding IAG 2007	23
	IAG 2007 Integration with ISA Server 2006	24
	Forefront UAG: The Next Generation of IAG 2007	25
	What's New in UAG?.....	25
	Aligning UAG with Security Needs	26
	Designing Network Protection.....	27
	When Do You Deploy UAG?	27
	When Do You Deploy TMG?	27
	Network Designs for TMG and UAG	28
	Summary.....	32
PART II	PLANNING FOR TMG	
Chapter 3	System Requirements	35
	Hardware Requirements	35
	Software Requirements	36
	General Recommendations.....	37
	Network Infrastructure	37
	Performance Monitoring	41
	Behavioral Monitoring	43
	Deploying in Virtual Environments	44
	Summary.....	45

Chapter 4	Analyzing Network Requirements	47
	Determining Your Traffic Profile	47
	Network Mapping	48
	Application Mapping	49
	Protocol Mapping	50
	TMG Deployment Options	51
	Edge Firewall	52
	Back Firewall	52
	Single Network Adapter	52
	Domain Isolation	53
	Addressing Complex Networks	53
	Configuring TMG Networks	54
	Understanding How Name Resolution Impacts TMG.	58
	Reviewing How Windows Resolves Names	58
	Recommendations for DNS Configuration on TMG	59
	Side Effects of DNS Issues	62
	DNS Cache in TMG	63
	Summary.	64
Chapter 5	Choosing the Right Network Topology	65
	Choosing the Network Template	65
	Edge Firewall Network Template	66
	3-Leg Perimeter Network Template	67
	Back Firewall Network Template	68
	Single NIC Network Template	69
	Examining High Availability.	71
	Designing High Availability for Publishing Rules	76
	Designing High Availability for Access Rules	80
	Joining the Firewall to a Domain or Workgroup	82
	Summary.	85

Chapter 6	Migrating to TMG	87
	General Considerations	87
	Go No Further Until You Understand This!	87
	Base Software	88
	Service Level	88
	If It Breaks	89
	Practice, Practice, Practice!	89
	Scenarios	90
	Publishing	90
	Dial-In VPN	91
	Site-to-Site (S2S) VPN	92
	Proxy	92
	Common Points	94
	Example Checklists	96
	Example Migration from ISA 2006 SE to TMG 2010 EE Forward	
	Proxy Scenario	99
	Summary	105
 Chapter 7	 Choosing a TMG Client Type	 107
	Web Proxy Client	107
	How the Web Proxy Client Works	109
	Server-Side Configuration	111
	When to Use the Web Proxy Client	112
	SecureNET Client	113
	How the SecureNET Client Works	115
	Name Resolution for SecureNET Clients	115
	SecureNET Client Advantages	117
	SecureNET Client Disadvantages	118
	Forefront TMG Client	119
	Winsock: A Primer	119
	Winsock Service Providers	122
	The TMGC as a Layered Service Provider	125
	TMGC Configuration Data	126
	Example Winsock Usage without TMGC	130

Winsock Usage with the TMGC	131
Web Proxy Client with TMGC	132
TMG Client Authentication	132
Choosing the Right Client for Your Environment	132
Ease of Deployment	132
Support for Heterogeneous Operating Systems	133
Protocol Support	133
Authentication Requirements and User- or Group-Based Access Control	133
Security	133
Summary.....	137

PART III IMPLEMENTING A TMG DEPLOYMENT

Chapter 8 Installing TMG	141
Final Considerations Before Installing TMG	141
Additional Recommendations	142
Installing TMG MBE	145
Manual Installation	146
Installing TMG 2010	156
Manual Installation	156
Unattended Installation	168
Summary.....	168
Chapter 9 Troubleshooting TMG Setup	169
Understanding Setup Architecture	169
Setup Goals	169
Setup Architecture	170
Setup Process	172
Setup Options	172
Applying Security Updates and Service Packs	173
Installing TMG with Updates	174
What to Look for When Setup Fails	174
Understanding the Setup Log Files	175

Reading Log Files	176
Setup Failed—Now What?	181
Summary.....	184

Chapter 10 Exploring the TMG Console 185

TMG Medium Business Edition.....	185
Monitoring	186
Update Center	187
Firewall Policy	188
Web Access Policy	188
Networking	191
System	191
Updates for TMG 2010.....	192
Monitoring	193
Firewall Policy	194
Web Access Policy	194
E-Mail Policy	194
Intrusion Prevention System	196
Networking	197
Logs and Reports	199
Update Center	199
New Wizards	199
The Getting Started Wizard	200
The Network Setup Wizard	201
The System Configuration Wizard	202
The Deployment Wizard	202
The Web Access Policy Wizard	203
The Join Array and Disjoin Array Wizards (TMG 2010 only)	203
The Connect to Forefront Protection Manager 2010 Wizard (TMG 2010 only)	204
The Configure SIP Wizard (TMG 2010 only)	205
The Configure E-Mail Policy Wizard (TMG 2010 only)	205
The Enable ISP Redundancy Wizard (TMG 2010 only)	206
Summary.....	206

Contents xi

Chapter 13 Configuring Load-Balancing Capabilities 263

Multiple Paths to the Internet.	263
What Is ISP Redundancy?	263
How ISP Redundancy Works	265
Link Availability Testing	265
Implementing ISP Redundancy	267
Planning for ISP-R	267
ISP-R Constraints	268
Enabling ISP-R	269
Failover Mode	269
Load-Balancing Mode	276
Understanding and Implementing NLB	284
NLB Architecture	285
Considerations When Enabling NLB on TMG	288
Configuring NLB on TMG	293
Post-Installation Best Practices	298
Considerations When Using TMG NLB in Virtual Environments	300
Troubleshooting NLB on TMG	301
Summary.	306

Chapter 14 Network Inspection System 307

Understanding Network Inspection System	307
Implementing Network Inspection System	309
Configuring NIS	311
Customizing Individual Signatures	316
Monitoring NIS	319
NIS Update	322
IPS Compared to IDS	322
Implementing Intrusion Detection.	323
Configuring Intrusion Detection	324
Configuring DNS Attack Detection	326
Configuring IP Preferences	327

Configuring Flood Mitigation	330
TMG Preconfigured Attack Protection	337
Summary.	341

PART V TMG AS YOUR CACHING PROXY

Chapter 15 Web Proxy Auto Discovery for TMG 345

WPAD as Protocol and Script	345
WPAD Protocol	345
WPAD Script	352
Configuring Automatic Discovery in the Network	364
Preparing for Automatic Discovery	365
Configuring Client Applications	374
Configuring Internet Explorer for Automatic Discovery	375
Automatic Proxy Cache	379
Troubleshooting Issues with Auto Discovery and IE	381
Configuring TMG Client for Automatic Discovery	381
Configuring Windows Media Player	382
Using AutoProxy in Managed Code	384
Summary.	385

Chapter 16 Caching Concepts and Configuration 387

Understanding Proxy Cache	387
How Caching Works	388
Cache Storage	389
Caching Scenarios	390
Cache Rules	391
Caching Web Objects	392
Caching Compressed Content	393
Monitoring Cache	394
Cache Array Routing Protocol (CARP)	395
How CARP Works	396

Chapter 18 URL Filtering	465
How URL Filtering Works	465
Components Involved in URL Filtering	469
Configuring URL Filtering	470
Global URL Filtering Configuration	472
Rule-Based URL Filtering Configuration	475
Testing URL Filtering	476
URL Category Overrides	477
Update Center	478
How Update Center Works	479
Configuring Update Center	481
Summary.	485
 Chapter 19 Enhancing E-Mail Protection	 487
Understanding E-Mail Threats	487
E-Mail Attack Methods	488
How SMTP Protection Works in TMG	490
Configuring SMTP Protection on TMG	493
Running the E-Mail Protection Wizard	494
Configuring Spam Filtering	502
Configuring Virus and Content Filtering	518
Summary.	527
 Chapter 20 HTTP and HTTPS Inspection	 529
The Web Proxy Application Filter.	529
Troubleshooting Web Proxy Traffic	
in TMG	532
HTTP Filter	533
Configuring HTTPS Inspection	534
Configuring HTTPS Inspection	538
Common HTTPS Inspection Errors	548

Troubleshooting Publishing Rules	647
Web Publishing Rules	647
Web Publishing Test Button	656
Non-Web Publishing Rules	657
Summary.	660
Chapter 23 Publishing Microsoft Office SharePoint Server	661
Planning to Publish SharePoint.	661
Security Considerations	662
Authentication	663
Alternate Access Mapping	664
Configuring SharePoint Publishing	665
Troubleshooting	689
Review Your Publishing Rule First	689
Summary.	696
Chapter 24 Publishing Exchange Server	697
Planning	697
Understanding Exchange Server Roles	697
Planning Client Access	698
Certificates	699
Authentication	700
Using the Wizards	702
Capacity Planning	703
Specific Client Considerations	706
Configuring Exchange Client Access through Forefront TMG	707
Troubleshooting	719
General Troubleshooting Rules	720
Exchange ActiveSync (EAS) and Office Mobile Access (OMA)	721
Outlook Web Access (OWA)	721
Exchange Web Services (EWS)	723

Outlook Anywhere (OA)	724
Using the Test Rule Button	725
Summary.....	730

PART VIII REMOTE ACCESS

Chapter 25 Understanding Remote Access 733

Understanding VPN Concepts	733
Tunnel Types	734
Protocols	734
Authentication	735
VPN Technology Comparison	736
Planning VPN Access	737
Selecting the VPN Protocol	738
Hardware Requirements	739
Authentication	741
VPN Access Policy	741
Supportability	742
NAP Integration.....	743
Considerations When Planning NAP Integration	745
Summary.....	745

Chapter 26 Implementing Dial-in Client VPN 747

Configuring VPN Client Access.....	747
Configure VPN Client Access with NAP Integration	756
Configuring Forefront TMG for NAP Integration	758
Configuring NPS to Use Forefront TMG as a RADIUS Client	762
Configuring VPN Client Access Using SSTP	763
Planning SSTP	766
Enabling SSTP on Forefront TMG	767
Changing Client Configuration	770
Summary.....	771

Chapter 27 Implementing Site-to-Site VPN	773
Configuring L2TP Over IPsec Site-to-Site VPN	774
Configuring PPTP Site-to-Site VPN	782
Troubleshooting VPN Client Connections	788
PPTP	788
L2TP over IPsec	790
SSTP	792
Common Errors and Likely Causes	793
Summary	794

PART IX LOGGING AND REPORTING

Chapter 28 Logging	797
Why Logging Is Important	797
New Firewall and Web Proxy Log Fields	798
Configuring TMG Logging	800
Common Logging Options	800
Log File and Disk Space Controls	803
SQL Express	804
SQL Database	805
Local Text Logging	807
Logging Queue	809
Logging Best Practices	809
Collecting Information about Your Environment	810
Logging Options	810
General Guidelines	812
Summary	815
 Chapter 29 Enhanced NAT	 817
Understanding Enhanced NAT	817
Configuring Enhanced NAT	820
Troubleshooting Enhanced NAT	826
Summary	828

Chapter 30 Scripting TMG **829**

Understanding the TMG Component Object Model (COM)	829
Forefront TMG COM hierarchy	830
New COM Elements in TMG	831
Administering TMG with VBScript or JScript	834
TMG Scripting Best Practices	834
TMG Task Automation Example	836
Administering TMG with Windows PowerShell	842
Windows PowerShell Automation Examples	845
Summary	848

PART X TROUBLESHOOTING

Chapter 31 Mastering the Art of Troubleshooting **851**

General Troubleshooting Methodology	851
You've Defined the Problem—What's Next?	853
Time to Analyze the Data	854
Got It, Now I'm Going to Fix It!	854
Troubleshooting Tools	855
TMG Troubleshooting Tab	858
Best Practices Analyzer	860
Network Monitor	861
Performance Monitor	861
Windows Event Logs	862
Putting It All Together	862
Real Life Case Study	862
Summary	868

Chapter 32 Exploring HTTP Protocol **869**

Understanding the HTTP Protocol	869
HTTP Transaction	870
How HTTP Authentication Works	874
Rules of the Game	874
HTTP Authentication in Action	876

Understanding HTTPS	884
Negotiation Phase	885
Client Acknowledgement	888
Server Acknowledgement	889
Summary.....	890

Chapter 33

Using Network Monitor 3

for Troubleshooting TMG

891

Using Network Monitor to Capture Traffic.	891
Data Gathering with Network Monitor	892
Reading a Network Monitor Capture	897
Troubleshooting TMG Using Network Monitor	903
Summary.....	909

<i>Appendix A: From Proxy to TMG</i>	911
<i>Appendix B: TMG Performance Counters</i>	937
<i>Appendix C: Windows Internet Libraries</i>	967
<i>Appendix D: WPAD Script CARP Operation</i>	973
<i>Index</i>	981

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Foreword

As the Product Unit Manager for the Forefront Threat Management Gateway (TMG) 2010 release, I was able to take advantage of a unique opportunity to change the industry regarding how we protect small business users and enterprise customers when connecting to the Internet in a world of ever-evolving threats, malicious software, and dynamic criminal activities. It was a challenge I could not pass up and I jumped at the opportunity to see how we could simplify the secure Web gateway (SWG) experience for customers and still provide the flexibility and security that hardcore security professionals have grown to love with the existing Internet Security and Acceleration (ISA) Server platform.

TMG has introduced a new era not only for Microsoft but also for the industry in how we create a comprehensive network protection solution for both small and large enterprise customers. Customers have told us that they love the Microsoft infrastructure integrated firewall and proxy that allows configuration and management using the tools and management infrastructure they are familiar with, such as Active Directory. But as we saw the threats and the workforce evolve, we realized that our customers needed something more to protect their users when accessing the Internet.

I wish I could summarize the full set of capabilities and potential in a short foreword for this book, but it proved to be impossible. The simple answer comes in the product name itself: Threat Management Gateway. The name deservedly implies the dynamic and integrated nature of the product and its extensible capability as it integrates with the Forefront Protection Suite. When you put it all together, the product really has six unique value propositions that emphasize our comprehensive approach to network protection:

- **Enforce network policy access at the edge** (Firewall)
- **Protect users from Web browsing threats** (Web Client Protection)
- **Protect users from e-mail threats** (E-mail Protection)
- **Protect desktops and servers from intrusion attempts**
(Network Intrusion System)
- **Enable users to remotely access corporate resources**
(VPN, Secure Web Publishing)
- **Simplify management** (Deployment)

In the end, the quality and the value proposition of the product speak for themselves. Throughout the beta program, we have had more downloads and production deployments than all the other betas of the ISA platform combined. The breadth of the new features has driven new customers and new deployments never possible with the ISA product line. On the firewall side, we have added key components such as VoIP traversal (SIP), Enhanced NAT, and ISP Link Redundancy. Combined with our NAP (Network Access Protection) integration with the VPN functionality, the firewall and remote access capabilities are richer than ever. On the Web client protection area, we now have integrated URL filtering, HTTP anti-virus/spyware scanning, and HTTPS forward inspection. The new secure e-mail relay deployment option enables a hardened edge-based anti-virus and anti-spam solution not previously available. And last but not least, the fully integrated and new Forefront Network Inspection System (NIS) has changed the game of network intrusion prevention and detection. Not only does the NIS provide the capability for administrators to provide threat management in the face of zero-day attacks, but it also enables security assessment and responses when deployed in conjunction with the Forefront Protection Suite.

What's next for the future of secure Web gateways and the threat landscape? If I were to be an oracle and predict the future, I would expect first that the trend of more complex malware and malicious attacks will continue to grow in volume and in criminal intent. I would also suspect that we will see a demand from the marketplace for further integration of information protection and control (IPC) with access and protection. We will see consolidation not only of solutions, but we'll also see the management and policy capabilities being integrated and unified across solution verticals. I believe TMG 2010 will be a product foreshadowing the future when it comes to network and virtualized datacenter protection.

In summary, this book is a must-have for the Forefront Threat Management Gateway administrator—it embodies the core of the product team development knowledge, the best practices from the Microsoft consultants around the world, and the learning from our customer deployments to date, and it distills this all into a one-stop resource kit of knowledge. Jim Harrison is known throughout Microsoft and the broader industry as the foremost ISA—and now TMG—expert. His in-depth understanding of the product internals combined with real-world deployment and operational experience provide a perspective unlike any other expert in the community. Yuri Diogenes and Mohit Saxena have not only been on the front lines of the top ISA deployments around the world, but have also been on the forefront (no pun intended) of the TMG beta program. Their firsthand guidance and best practices will help you ensure a smooth and easy deployment

by avoiding mistakes in advance and suggesting the most secure configuration from the start. Tom Shinder, a recognized Microsoft security professional and widely known ISA expert, brings his extended ISA experience to bear as a valued technical reviewer for this book.

The availability of this book helps to achieve the goal that we set with the original inception of the TMG project: to enable customers to deploy protection easily in a cost-effective and manageable way to achieve their security and application-protection requirements in an ever-changing threat landscape. I believe we have achieved that goal with our upcoming release and with security experts such as Jim, Yuri, and Mohit evangelizing the knowledge.

David B. Cross
Product Unit Manager
Microsoft Corporation

Acknowledgments

This book took more than a year to write; starting in April 2008 with our final content submission in September of 2009. Although the authors get lots of credit for a book, there can be little doubt that we could not have even begun, much less completed this book, without the cooperation (not to mention the permission) of an incredibly large number of people. We'd like to take a few moments of your time here to express our gratitude to the folks that made it all possible.

From “The Collective”

To Dr. Tom Shinder for adding his deep and broad technical and writing experience as a technical reviewer. Much of what you read herein is the result of Tom's willingness to ask us, “Wachootawkinbout, Willis?”

To the folks at Microsoft Press who made the process as smooth as they possibly could: Carol Vu and her team of crack editors, Karen Szall, and Martin DelRe, who helped us get this project off the ground.

To David Cross and the Forefront Edge marketing team, who approved and supported us in this effort, and especially to David for writing the foreword.

To the TMG Core and CS teams, who responded immediately and in painstaking detail to our unending stream of e-mails. You folks built an extremely fine product and we sincerely hope we did your efforts justice.

To Bala Natarajan and the whole TMG TAP team who continually asked us, “Are you dealing with this in your book?” (causing several chapter rewrites), but never failed to make the book better in the process.

To Paul Long and the Network Monitor Team for producing Network Monitor and reviewing Chapter 33, “Using Network Monitor 3 for Troubleshooting TMG.”

To Mark Stanfill for assisting during the creation of the Windows PowerShell script—your assistance was very much appreciated.

To the Security Content Review Board participants: We may not always agree with what you offer, but we always took your review comments seriously.

From Jim

First and foremost, to my wife, Lois, who in an apparent fit of extreme silliness responded, “Sure—go ahead!” when I asked her permission to collaborate with Yuri and Mohit on this book. Neither she nor I had a clue what lay before us, but she never wavered and more than anything else her support helped keep me on track.

To Yuri and Mohit, who must have wondered if “my head was with me all day” (three social points for that quote) when they read some of my review comments. You guys made this far easier and much more fun than it might have been otherwise. I’m all little-girl-giggly to see my name printed alongside yours on this book.

To Tom: It took me almost 10 years (yes, we’ve been “ISA-lated” that long), but I finally had a chance to give you “your props” in my book. Thanks so much for helping—the book is that much better as a result of your participation!

To “Da Boyz”; Tom, Tim (Thor), Steve, and Greg—there’s nothing like a group of solid bros that’s willing to call me to task for my cranial effluvium.

From Yuri

Above all, thanks to God for blessing my life and leading my way. I also couldn’t have even thought about writing this book if I didn’t have such a great family. They have always supported me and understood my long days away working on this long project: I love you, Yanne and Ysis. Thanks to my wife, Alexsandra, for all your comprehension and love. Without you this wouldn’t be possible.

To Jim and Mohit, I have a simple sentence to define those months working on this project with y’all: It was an honor to share so many great moments. Each of you contributed to my personal growth with your thoughts, advice, and guidance. Without a doubt these long months writing this book were worth it because of this amazing partnership that we had. The same applies to Tom, who jumped on this project at the right moment and used his vast writing experience in guiding all of us to write this content better.

Last but not least I would like to say thanks to all my friends from Microsoft CSS Security (Texas, North Carolina, Washington, EMEA, and India) for sharing your experiences every day and to my direct managers for supporting my passion to write and giving me so many opportunities to do so. To Nathan Bigman: You were responsible for this writing dream that became true. To my buddies Alexandre Hollanda and Mohit Kumar: Thanks, guys, for always being there when I need you.

From Mohit

First and foremost I would like to thank my wife, Anusha, for being extremely supportive during the time I was working on this book and for being my strength during times when I really felt I couldn't write anymore. I still remember times when I was up late into the night, trying to meet deadlines for the book along with my regular work and feeling completely frustrated. A cup of hot coffee along with a gentle reminder from her that no matter how much hard work it was I could still do it took all the frustration away. I really couldn't have done this without her love and support and without my little puppy, Mojo, who stayed up with me as long as I worked. I would also like to thank my parents and my brother, who have always inspired me to take on more challenges in life and remind me that the only change that is constant in life is knowledge, and by sharing your knowledge you gain more.

To Jim and Yuri: I still remember the day when I jokingly mentioned the idea to Yuri. I understood later that joking about any idea about writing to Yuri is always dangerous. The whole idea of writing a book was a dream that soon turned into reality when Jim joined us. I will always be thankful to you two for helping this dream come true for me. Thank you for bearing with me when I was late on the schedule (which I always was) and for always being there to cover for me whenever I couldn't complete my part. We would have never been able to complete this book so soon if it hadn't been for Yuri making sure we stuck to our deadlines and for Jim making sure to correct me technically if I had wandered off into my own ideas. A big thank you to Tom for helping us make this book a masterpiece with his participation and guidance.

Finally, I would like to thank all my teammates in Bangalore, Charlotte, Las Colinas, and Redmond along with my managers for being supportive of my passion to write this book. Thanks to Bala Natarajan, Dan Herzog, Mohit Kumar, and Tarun Sachdeva for always being patient with me and helping me with all my questions, but above all being great friends.

Introduction

Welcome to the *Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion*. This book was written over the course of more than a year to help you design, deploy, and maintain TMG in multiple scenarios as well as to help you understand the history and design goals of TMG. The functionality descriptions and examples in this book are based on actual deployment and testing in the authors' labs, so you can rest assured that what we describe is a demonstrated fact, not simply a "feature description."

Forefront TMG was designed and tested to provide the best possible security for Internet access for your users and to provide you with the means to more easily understand and manage the ever-increasing Internet threat landscape. Network Inspection, HTTPS Inspection, Enhanced Malware Protection, and URL Filtering are all designed to help you provide greater security for your users. The built-in troubleshooting tools are included to help you keep your TMG deployments running at peak performance and effectiveness.

The Target Audience

The person we tried to keep in mind while writing this book is someone with at least a year of experience deploying and troubleshooting networks with at least 2 to 10 routed subnets. Ideally, you would have some experience configuring switches, routers, and basic firewalls and also have had some experience with ISA Server 2004 or ISA Server 2006. You should also have some basic understanding of common Internet protocols such as HTTP, SMTP, IMAP, IPsec, PPTP, and so on, and be familiar with the OSI network model.

This book is written by technical people for technical people; the goal is to inform and educate. The primary product focus of the book is TMG 2010. ISA Server is included to provide historical comparison and to illustrate improvements TMG offers over ISA Server. TMG (MBE), IAG, and UAG are included to illustrate differences between TMG 2010 and these other products and to help you decide which product best serves your needs.

One thing to bear in mind as you work your way through this book is that many of the descriptions and screen shots were written using pre-release versions of the product—from early beta up to the first release candidate. We performed a review of all chapters just before TMG was released in order to ensure that the information and screen shots were as current as we could possibly make them.

Organization and Usage

In general, we've organized the book so that you get some background on a feature set as well as introducing the feature to you. With the exception of those chapters that required reevaluation as the product evolved over the past year, we were able to keep with the planned layout. You may notice those that seem out of place as you use the book.

We wrote this book with an eye toward functional usage. The first section provides an introduction to TMG as a single product and in the context of other Forefront Edge products. Each section collects chapters into functional groups that are related by an overarching concept, such as protected clients, publishing, and so on, and within each chapter that addresses specific action, we've tried to include some basic troubleshooting methodology and examples.

Part 1 A New Era for the Microsoft Firewall

Part 1 includes discussions on TMG features, design goals, and their relationship to the Microsoft Forefront Edge product line.

Chapter 1 What's New in TMG

Chapter 1 summarizes the design goals and scenarios for TMG in comparison to ISA Server, Internet Access Gateway (IAG), and Universal Access Gateway (UAG).

Chapter 2 What Are the Differences Between TMG and UAG?

Chapter 2 details the design goals and scenarios for TMG in comparison to Universal Access Gateway (UAG). It provides comparisons between IAG and UAG for historical reference.

Part 2 Planning for TMG

Part 2 includes discussions on planning for TMG deployments, including product requirements, client traffic considerations, and virtual deployments.

Chapter 3 System Requirements

Chapter 3 details and discusses the hardware and software requirements for TMG. This chapter also covers considerations for deploying on a virtual environment.

Chapter 4 Analyzing Network Requirements

Chapter 4 discusses the methodology for determining the traffic profile and client load for TMG deployments. This chapter also addresses distributed and remote traffic paths related to client traffic profiles.

Chapter 5 Choosing the Right Network Topology

Chapter 5 discusses the methodology for determining the correct network topology for TMG. This chapter also deals with the question of domain membership versus workgroup deployments for TMG as well as high-availability scenarios and solutions.

Chapter 6 Migrating to TMG

Chapter 6 discusses how to plan, coordinate, and test migrating from an ISA Server deployment to a Forefront TMG deployment.

Chapter 7 Choosing a TMG Client Type

Chapter 7 discusses the various client request types supported by TMG as well as the deployment choices that impact the use of these clients.

Part 3 Implementing a TMG Deployment

Part 3 covers installing and configuring TMG Medium Business edition and TMG 2010 and provides an introduction to the new management console.

Chapter 8 Installing TMG

Chapter 8 covers installing TMG MBE separately from Windows Essential Business Server as well as installing TMG 2010. This chapter provides checklists that refer to concepts provided in the planning chapters.

Chapter 9 Troubleshooting TMG Setup

Chapter 9 discusses the methodology for troubleshooting TMG setup failures. This chapter provides details on how the setup mechanisms are constructed and how they interrelate as well as guidance on using the setup logs to solve TMG installation problems.

Chapter 10 Exploring the TMG Console

Chapter 10 introduces you to the TMG management MMC and provides comparisons to ISA 2006 and TMG Medium Business edition (MBE). This chapter also outlines new wizards provided by TMG.

Part 4 TMG as Your Firewall

Part 4 includes discussions on TMG network concepts as well as configuring and troubleshooting network and access rules. This section also includes a discussion on NIS.

Chapter 11 Configuring TMG Networks

Chapter 11 discusses TMG logical network configurations and the impact these choices have on TMG behavior. This chapter includes a basic discussion on IP routing to help you understand how TMG networks operate.

Chapter 12 Understanding Access Rules

Chapter 12 discusses how the TMG policy engine processes traffic in the context of access rules and includes guidance on basic troubleshooting.

Chapter 13 Configuring Load-Balancing Capabilities

Chapter 13 discusses load-balancing concepts in general, including Network Load Balancing (NLB), DNS Round-Robin (DNS-RR), and ISP Redundancy (ISP-R). This chapter also provides comparisons of each solution and how they interact.

Chapter 14 Network Inspection System

Chapter 14 discusses how TMG implements Generic Application Protocol Analysis (GAPA) in the Network Inspection System (NIS) to protect computers that send their traffic through TMG.

Part 5 TMG as Your Caching Proxy

Part 5 introduces general caching concepts as well as TMG caching mechanism and controls.

Chapter 15 Web Proxy Auto Discovery for TMG

Chapter 15 covers WPAD as the discovery protocol and the configuration script provided by TMG. This chapter includes general network requirements and steps to ensure proper WPAD behavior.

Chapter 16 Caching Concepts and Configuration

Chapter 16 discusses Web caching as implemented within TMG. This chapter includes TMG cache configuration and troubleshooting methodology.

Part 6 TMG Client Protection

Part 6 introduces protection mechanisms provided by TMG for clients in protected networks.

Chapter 17 Malware Inspection

Chapter 17 discusses TMG Malware Inspection, including how to configure it for your organization's needs and how to produce reports that summarize EMP detection actions.

Chapter 18 URL Filtering

Chapter 18 discusses URL Filtering concepts, including the relationship with Microsoft Reputation Services (MRS). You'll also learn how to configure URLF to meet your organization's requirements.

Chapter 19 Enhancing E-mail Protection

Chapter 19 discusses the threat landscape presented by e-mail and how TMG works with Exchange Edge and Forefront Protection 2010 for Exchange Server to minimize the threats presented to your organization.

Chapter 20 HTTP and HTTPS Inspection

Chapter 20 discusses how TMG handles inspection for HTTP traffic and how the new HTTPS Inspection (HTTPSi) feature helps to improve this functionality.

Part 7 TMG Publishing Scenarios

Part 7 discusses publishing concepts in general as well as specific publishing scenarios.

Chapter 21 Understanding Publishing Concepts

Chapter 21 discusses the functional concepts related to publishing scenarios. This chapter also discusses how to properly plan your publishing scenarios and the resulting TMG policy configuration.

Chapter 22 Publishing Servers

Chapter 22 discusses how to publish Web and non-Web services to best take advantage of TMG functionality and security mechanisms.

Chapter 23 Publishing Microsoft Office SharePoint Server

Chapter 23 discusses how to plan and publish Windows SharePoint services. This chapter includes publishing concepts specific to SharePoint, publishing steps, and troubleshooting hints.

Chapter 24 Publishing Exchange Server

Chapter 24 discusses the concepts and methodology for publishing Exchange mail services, such as Outlook Web Access and SMTP. This chapter also includes discussions about proper certificate construction and installation as well as troubleshooting guidance.

Part 8 Remote Access

Part 8 discusses remote access concepts including the protocols involved. This part also details configuring TMG for dial-in and Site-to-Site VPN access.

Chapter 25 Understanding Remote Access

Chapter 25 discusses VPN concepts, including detailed, comparative discussions on various VPN tunnel technologies and related protocols. Network Access Protection (NAP) integration is also introduced in this chapter.

Chapter 26 Implementing Dial-in Client VPN

Chapter 26 includes detailed instructions on how to configure TMG to provide dial-in VPN access using classic VPN, SSTP, and NAP.

Chapter 27 Implementing Site-to-Site VPN

Chapter 27 includes detailed instructions on how to configure TMG to support Site-to-Site VPN networks using classic L2TP/IPsec and PPTP. This chapter also includes troubleshooting guidance for common issues.

Part 9 Logging and Reporting

Part 9 discusses logging, reporting, administrative scripting for TMG, and Enhanced NAT.

Chapter 28 Logging

Chapter 28 discusses firewall logging in general as well as what TMG logging provides you. This chapter also includes discussions on logging best practices.

Chapter 29 Enhanced NAT

Chapter 29 discusses Enhanced Network Address Translation (ENAT) concepts, configuration, and troubleshooting.

Chapter 30 Scripting TMG

Chapter 30 provides a discussion of the TMG Component Object Model (COM) and changes to the COM since ISA 2006 and also provides scripting examples in VBScript, Jscript, and Windows PowerShell.

Part 10 Troubleshooting

Part 10 covers general troubleshooting, as well as techniques and tools useful for troubleshooting TMG scenarios.

Chapter 31 Mastering the Art of Troubleshooting

Chapter 31 discusses the habits and techniques understood by all good troubleshooters. This chapter includes discussions of problem recognition, methodology, and tools.

Chapter 32 Exploring the HTTP Protocol

Chapter 32 provides a detailed discussion on the HTTP protocol; the authentication methods it includes; and how adding Secure Sockets Layer (SSL) to the protocol changes client, proxy, and server expectations.

Chapter 33 Using Network Monitor 3 for Troubleshooting TMG

Chapter 33 uses Network Monitor 3 to discuss the concepts and methodology behind TMG troubleshooting using a network capture and analysis tool.

Appendices

The appendices include content providing expanded explanations as well as historical references.

Appendix A From Proxy to TMG

This section includes discussions on TMG features, design goals, and the relationship between TMG and the Forefront product line.

Appendix B TMG Performance Counters

This section includes discussions on TMG performance counters and how they may be used together and separately to monitor TMG behavior and identify problems as well as the need to scale up or out.

Appendix C Windows Internet Libraries

This section includes discussions on two Windows Internet libraries (WinInet and WinHTTP). We provide special considerations for each with regard to CERN proxy behavior and limitations.

Appendix D WPAD Script CARP Operation

This section includes a detailed discussion on the TMG CFILE and includes some test scripts for use by the TMG administrator to test client-side CARP behavior.

Terminology

While writing this book, we strove to maintain the standard terms in describing general networking concepts as well as specific technologies, mechanisms, and protocols. In particular, and because there is so much argument on this point, our use of the terms *firewall*, *server*, *computer*, and *proxy* are described below:

- **Firewall** This term may be used in reference to TMG in the context of its function as a firewall—a network entity that controls traffic flow between two or more unique networks.
- **Proxy** This term may be used in reference to TMG in the context of its function as a proxy server. This includes the following use cases:
 - CERN proxy (AKA forward proxy) and Web Publishing (AKA reverse proxy)
 - SOCKS proxy as defined in <http://en.wikipedia.org/wiki/SOCKS>
 - Winsock proxy (AKA TMG Clients) as described in <http://technet.microsoft.com/en-us/library/ee291341.aspx>
- **Server** This term may be used in reference to TMG in the context of any function normally provided by Windows Server mechanisms, such as file shares, authentication, and so on. This term may also be used to refer to TMG in the general sense, such as *array server* or *the TMG server*.

- **Computer** This term may be used in reference to TMG in the context of any physical or logical configuration related specifically to Windows or the underlying server hardware itself, such as CPU, memory, network interfaces, and so on.

Companion CD

The companion CD is a valuable addition to this book and includes the following items:

- Sample scripts written in Visual Basic Scripting edition (VBScript), Java Script (Jscript), or Windows PowerShell for TMG administration. These scripts can be used either as is or customized to meet your administrative needs.
- SOCKS parser for Network Monitor 3.3. Instructions for the use of this parser are included on the CD.
- An electronic version of the entire *Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion*.

Full documentation of the contents and structure of the companion media can be found in the Readme.txt file on the CD.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD. Visit <http://www.microsoftpressstore.com/title/9780735626386> to get your downloadable content. This content is always up-to-date and available to all readers.

System Requirements

You'll need the following hardware and software to work with the companion content included with this book:

- Microsoft Windows Vista, Windows Server 2008, or Windows 7. Server Core is not supported for TMG or these tools.
- Microsoft Forefront TMG (for server installation) or Remote Administration (for client operating systems).
- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor.
- 1 GB of available, physical RAM.
- Video (800 × 600 or higher resolution) monitor with at least 256 colors.
- CD-ROM or DVD-ROM drive.
- Microsoft mouse or compatible pointing device.
- Adobe Reader for viewing the eBook (Adobe Reader is available as a download at <http://adobe.com>).

Feedback and Support for This Book

Although we always strive for perfect content, the fact that humans are involved in the process from start to finish (no, really—we have flesh and bones and bad breath and everything) pretty much guarantees that we won't achieve that lofty goal. Because you will no doubt discover mistakes, or something we've said may raise more questions than answers, please feel free to contact us collectively at authors@mstmgbok.org. We will respond as soon as possible with an answer appropriate to the question or comment.

Every effort has been made to ensure the accuracy of this book and companion content. As corrections or changes are collected, they will be added to a Microsoft Knowledge Base article accessible via the Microsoft Help and Support site. Microsoft Press provides support for books, including instructions for finding Knowledge Base articles, at the following Web site:

<http://www.microsoft.com/learning/support/books/>

If you have questions regarding the book that are not answered by visiting the site above or viewing a Knowledge Base article, send them to Microsoft Press via e-mail to mspinput@microsoft.com.

Please note that Microsoft software product support is not offered through these addresses.

We Want to Hear from You

We welcome your feedback about this book. Please share your comments and ideas via the following short survey:

<http://www.microsoft.com/learning/booksurvey/>

Your participation will help Microsoft Press create books that better meet your needs and your standards.

NOTE We hope that you will give us detailed feedback via our survey. If you have questions about our publishing program, upcoming titles, or Microsoft Press in general, we encourage you to interact with us via Twitter at <http://twitter.com/MicrosoftPress>. For support issues, use only the e-mail address shown in the previous section.

Choosing the Right Network Topology

- Choosing the Network Template **65**
- Examining High Availability **71**
- Joining TMG to a Domain or Workgroup **82**
- Summary **85**

You may have the challenging task of designing the network infrastructure TMG will serve. If this is the case, or even if you're just trying to decide which TMG network topology best applies to your network infrastructure, you'll want to read through this chapter carefully so that you make the right decision the first time. Changing this decision after deploying TMG can present some difficult challenges.

Choosing the Network Template

After establishing your traffic profile and identifying the IP address ranges that belong to your networks, it is time for you to determine which network template you will apply to TMG. The template you choose should match your current TMG configuration and satisfy your network needs.

In Chapter 4, "Analyzing Network Requirements," you identified TMG placement considerations, and during this process you saw that TMG can be placed at the edge of your network as a front-end firewall, behind another firewall in a back-end firewall configuration, or as a single NIC Web proxy (forward and reverse Web proxy). TMG network templates can assist you in reflecting the physical configuration into a logical firewall or Web proxy configuration. TMG includes four network templates:

- Edge Firewall
- 3-Leg Perimeter
- Back Firewall
- Single Network Adapter

You can choose the network template when you run the Getting Started Wizard by choosing Configure Network Settings. But before we apply the template it is important to understand what each template does.

Edge Firewall Network Template

You need a firewall on the edge regardless of your deployment; this adds the first layer of protection for your internal assets. By using the Edge Firewall network template for this scenario, you apply a configuration that reflects the main goal of your edge TMG placement.

This template assumes that you have two interfaces: one connected to the internal network and one connected to the external network. Usually the external interface is the one connected directly to the Internet (through a router for instance), but it can also be behind another firewall or NAT device. Most often, the external interface is the NIC configured with a default gateway.

When you run the Getting Started Wizard, choose the Edge Firewall template, as shown in Figure 5-1.

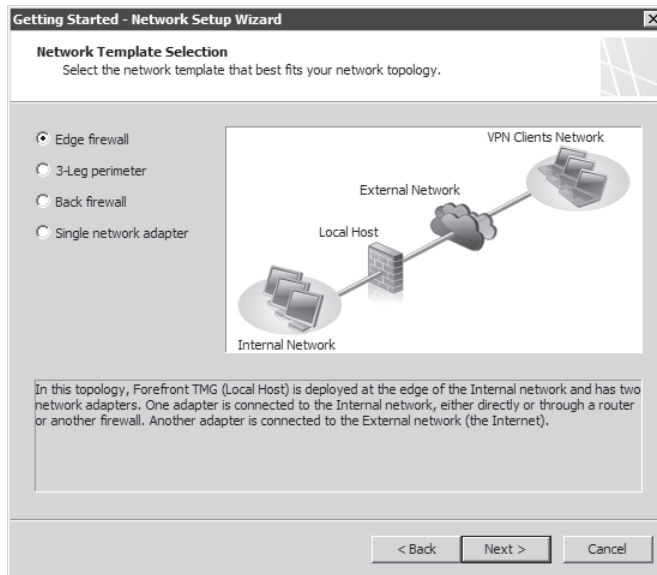


FIGURE 5-1 The Getting Started Wizard—Edge Firewall template selection

This template provides the following benefits:

- TMG blocks all unauthorized attempts to gain access to the default Internal Network from the default External Network.
- TMG hides the default Internal Network from the outside.

- You have the ability to provide secure access to internal servers by publishing them.
- The template carries little overhead and has an easy configuration.

MORE INFO For more information about how to run the Getting Started Wizard, read Chapter 4 of this book.

3-Leg Perimeter Network Template

The 3-Leg Perimeter template can assist you in implementing a perimeter network, also known as demilitarized zone, or DMZ. This perimeter network is used to securely expose resources that are shared by users coming from untrusted networks (such as the Internet) and trusted networks (TMG-protected networks).

This template involves setting up TMG with three network interfaces. One network adapter is connected to the Internet (external network), one is connected to the internal network, and the third is connected to a perimeter network. The 3-Leg Perimeter option is not available if you have fewer than three NICs installed on TMG.

When you run the Getting Started Wizard you can choose the 3-Leg Perimeter template, as shown in Figure 5-2.

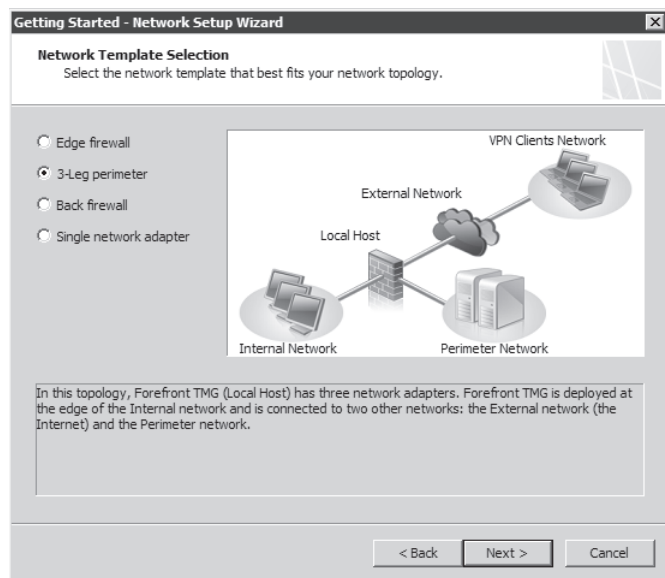


FIGURE 5-2 The Getting Started Wizard—3-Leg Perimeter template selection

By selecting this template in the Getting Started Wizard, you will have to specify later which adapter is connected to the perimeter as shown in Figure 5-3.

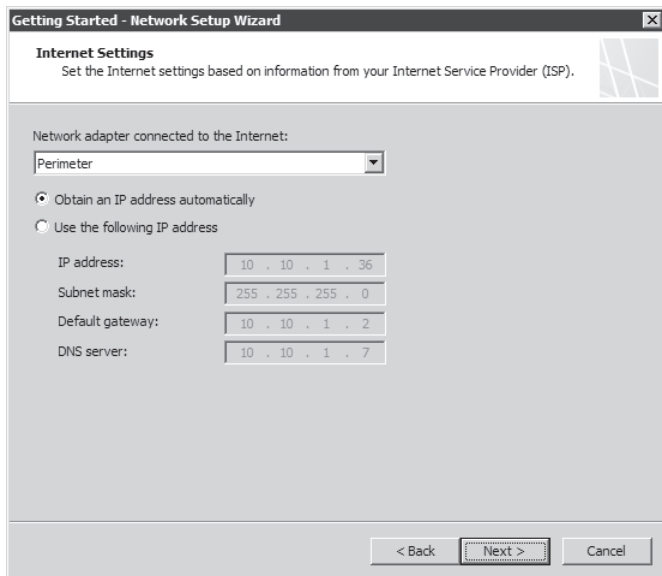


FIGURE 5-3 Selecting the perimeter adapter

During this selection you need to specify whether the IP addresses used on the perimeter network are public or private. This is a key determination because it also affects the network relationship between the perimeter network with the default Internal and External networks. The perimeter network usually uses private IP addresses, which is the typical scenario because you want to hide the real IP address of the resource from Internet.

This template provides the following benefits:

- It protects the default Internal Network from external attacks.
- Allows you to securely publish services to the Internet by placing them in a perimeter zone.
- External users can access resources located in the perimeter network while still being prevented from accessing internal resources.

Back Firewall Network Template

Scenarios involving the Back Firewall template include the deployment of TMG in between a perimeter network and the default Internal network. TMG acts as the back-end line of defense for the internal resources. Another firewall is necessary between the external network and perimeter network. Use this scenario when you want to provide two lines of defense and also gain the following benefits:

- Granular access control
- Multiple layers of protection
- Separation of duties (Each firewall is responsible for different traffic profiles.)

When you run the Getting Started Wizard you can choose the Back Firewall template, as shown in Figure 5-4.

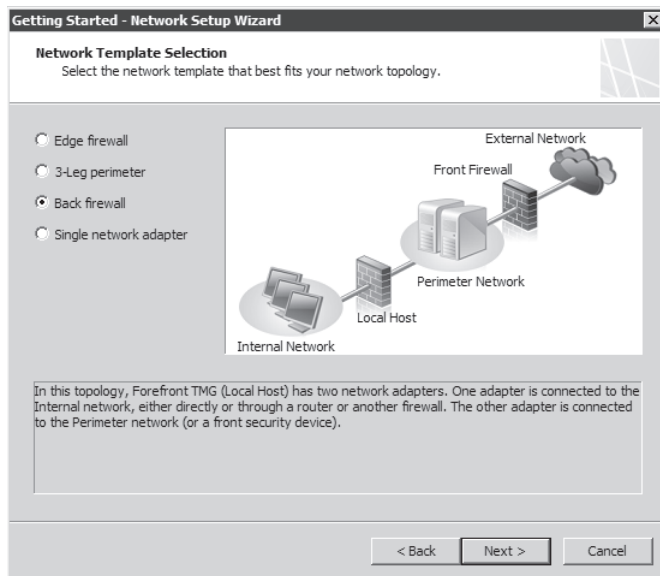


FIGURE 5-4 The Getting Started Wizard—Back Firewall template selection

When you select this template using the Getting Started Wizard, you have to specify which adapter is connected to the default Internal Network and which adapter is connected to the perimeter network.

Single NIC Network Template

You use the Single NIC template when you want to limit the firewall to one or more of the following roles:

- A forward Web proxy server
- A Web caching server
- A reverse Web proxy (Web publishing—HTTP/HTTPs, RPC over HTTPs, and FTP)
- A VPN remote-access client server

You cannot use a single NIC TMG to protect the edge of your network. The single NIC scenario assumes that TMG will provide these limited services and that another firewall will provide edge security.

The Single NIC template introduces a number of limitations to TMG functionality. The single NIC TMG has no concept of an external network, because it has only one network interface and the default gateway that connects you to anything beyond your own network lies on the same network card. Therefore, the only networks available are localhost (TMG itself) and internal. All firewall policies need to be created by using those elements.

Additionally, using the Single NIC template creates a number of unsupported scenarios, including:

- **Application filtering** Although the TMG has built-in application-layer inspection, the Single NIC template limits what can be inspected. Application-layer inspection is done only for HTTP/HTTPS and FTP over HTTP traffic.
- **Server Publishing** The Server Publishing feature requires two network interface cards (NICs); this template supports only a single NIC deployment.
- **TMG Client** TMG client requests are not supported.
- **SecureNET Client** SecureNET client requests are not supported.

Even if you configure a network adapter to use two or more IP addresses or you add a second network adapter and later disable it in an attempt to work around some of those limitations, this configuration still does not add support for the above scenarios.

When you run the Getting Started Wizard, you can choose the Single NIC template as shown in Figure 5-5.

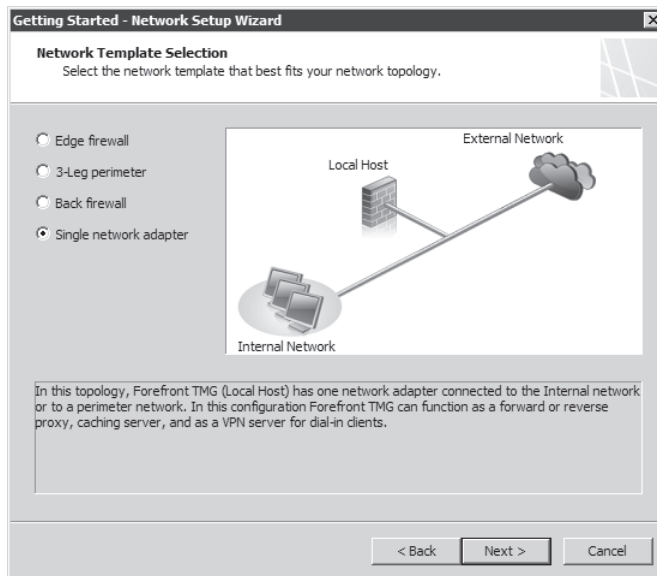


FIGURE 5-5 The Getting Started Wizard—Single NIC template selection

After you apply the single NIC template the following addresses are excluded from the network:

- 0.0.0.0
- 255.255.255.255
- 127.0.0.0 – 127.255.255.255
- 224.0.0.0 – 254.255.255.255



REAL WORLD Cannot Access Some Web Sites

The following real-world example is based on a support incident regarding a recent deployment of TMG using the Single NIC template. The user was trying to access a Web site that gave him access to a payroll system. Unfortunately, this company didn't really communicate how the Web site worked, and according to the basic manual the only traffic required was HTTPS (SSL).

The user was able to access the first page and log in to the system, but when he tried to retrieve data from the payroll system, the page never loaded completely. The user argued that TMG was at fault because everything worked fine when TMG was bypassed. We had to do some reverse engineering to understand how this application worked. By using Network Monitor 3.2 we were able to view the details of the client/server traffic and we could see that the application indeed used HTTPS, but it also tried to open some Winsock connections using a non-HTTP port.

That was the problem: to use this application, the customer needed support for both Web and non-Web protocols. To get support for non-Web protocols (and require client authentication), the user needed to use the TMG Client on his workstations to handle Winsock requests. But the problem was that the user was running a single NIC environment and the TMG Client requests are not supported in this configuration.

The bottom line was that the user had to add a second NIC and reconfigure TMG to use the Edge Firewall template. The lesson is that you really need to determine your traffic profile and define the type of traffic you need to support when you are purchasing a service from a third party. Make sure to ask what protocols are required. By defining this prior to implementing the application, you might avoid long support calls that end up being due to an unsupported scenario.

NOTE The Single NIC template can be very useful if you clearly understand the limitations it imposes. However, regardless of the template you choose, it is important to mention that you should not use more than one default gateway on the external interface. This is also an unsupported scenario and can cause connectivity problems for your Forefront TMG.

Examining High Availability

Implementing a highly available network service frequently means different things to different people depending on their experiences in the IT community. In general, all network and application administrators agree that the term *high availability* means "uninterrupted service availability to the user." In other words, if the service has to defer a user's traffic path from one server to another, the user should not be aware that this action has occurred.

For example, some network or application administrators consider the goals of load-balancing and failover/failback to be completely different tasks, but they usually agree that they can both be employed to provide a more robust service to the user. In fact, if you choose to use load-balancing and failover/failback in combination, it's in your best interest to deploy these mechanisms in a way that allows them to be compatible rather than conflicting. Otherwise, you could spend a great deal of your time chasing ghosts in the machine caused by conflicting traffic management mechanisms.

One thing all high-availability solutions have in common is that they try to use one or more aspects of the traffic definition to determine how the traffic should be handled in the course of traffic balancing across a server farm and in case of server failure. The use of one or more aspects of the conversation to control traffic flow is called *affinity*.

Most IP traffic is defined by a combination of five unique identifiers, known as a *5-tuple*:

- **Source IP address** The IP address of the sending host.
- **Destination IP address** The IP address of the receiving host.
- **Transport** The IP protocol (TCP, UDP, GRE, and so on) that carries the higher-level protocol, such as SSL or HTTP. Note that only TCP and UDP provide source and destination ports.
- **Source port** A number identifying the transport socket used by the sending host.
- **Destination port** A number identifying the transport socket used by the receiving host.

In network protocol layer order, the following list describes some common high-availability techniques:

- **Source IP affinity** High-availability solutions that use this technique build a map of the traffic flow in the context of the host IP addresses that started the conversation (the client). The primary advantage to this technique is that it guarantees all traffic from a specific IP address is always sent to a specific server, regardless of the higher-level protocols in use. This also represents the greatest disadvantage of this technique: When traffic from multiple clients is sourced from behind a remote NAT or proxy device, the source IP for all clients is likely to be the same. This is the primary traffic management method used by NLB. TMG offers IP affinity for Web Publishing Load Balancing (WPLB).
- **Source port affinity** This technique builds a map of the traffic flow in the context of the transport and source port. This is one method by which a high-availability mechanism can get around a case where multiple clients are behind a NAT or proxy device that makes them all appear as a single source IP. The primary advantage to this technique is that it is independent of the source or destination addresses. The primary disadvantage is that this technique can only be applied to protocols that make use of ports (TCP and UDP). Where protocols that do not use ports (such as GRE) are used, this method cannot be employed. When NLB is configured for *no affinity*, it is actually configured to use source port affinity.

- **SSL-ID affinity** SSL is a session layer protocol because it operates a layer above the transport protocols in the network protocol stack. Although it doesn't fall into the 5-tuple definition we described, it provides a statistically unique identifier that can be used to build the traffic flow map. The primary advantage of this technique is that it is a better identifier than IP addresses or ports, because it is cryptographically defined at the server side of the conversation and therefore unique to all traffic served by that host. The primary disadvantage to this technique is that although many third-party vendors use this, their management of the traffic in this context varies and occasionally conflicts when these techniques are used together. Neither TMG nor NLB support SSL-ID affinity.
- **HTTP cookie affinity** Because much of the traffic crossing the Internet is HTTP, and because HTTP offers the concept of cookies as a unique session identifier for the client application itself, many high-availability solutions make use of cookie affinity. TMG also offers this when configured for WPLB. The primary advantage to this technique is that it is independent of the lower-layer protocols and can be used to uniquely identify a user's browser session. This technique has a couple of disadvantages: The high-availability device must terminate SSL sessions; otherwise, it cannot insert the cookie in the response headers or read the cookies created by the server in the response headers. In addition, in some cases, such as Microsoft Office Outlook Anywhere and Terminal Services Gateway, cookies are not handled by the client application as the high-availability solution expects (if at all). TMG provides cookie affinity for WPLB; NLB does not support cookie-affinity.
- **DNS Round-Robin** This method takes advantage of the ability to define more than one IP address for a host name in a DNS zone. In most cases, when a client queries a host name for which multiple IP addresses are defined, the DNS server will respond with all of the IP addresses defined for that host. Depending on the capabilities and configuration of the DNS server, it may apply IP filtering or ordering according to the subnet structure it determines based on the requesting host's IP address.

IMPORTANT DNS Round-Robin functionality varies between DNS server implementations and is referred to as *netmask ordering*. You can read more about Microsoft DNS netmask ordering at <http://technet.microsoft.com/en-us/library/cc787373.aspx>.

Although not strictly a high-availability mechanism, this is a very cheap (almost free) method for providing client connection load-sharing and failover. Neither TMG nor NLB have any effect on DNS Round-Robin, although the combination of DNS RR with NLB can produce interesting (read: confusing) results and are best not used in combination.

IMPORTANT Although DNS Round-Robin is a very popular high-availability method because of its low cost and ease of deployment and management, it doesn't come highly recommended because its effectiveness is entirely dependent on how the client operating system or application handles such responses. A high-availability solution that depends almost entirely on client operating system or application behavior is not a high-availability solution that you can exert much influence over.

- **Bidirectional affinity** This affinity requires that the high-availability solution have a monitor and control point on opposite sides of the traffic path across a NAT device, and that both sides of this high-availability solution must intercommunicate to maintain proper traffic flow across it. NLB and some third-party high-availability solutions support this mechanism, although some of the third-party solutions require that you purchase duplicate units to have a functional bi-directional high-availability mechanism. The primary purpose of this mechanism is to ensure that traffic related to this connection is guaranteed to take the same path between the two endpoints. We discuss this in more detail in Chapter 8, “Installing TMG.”

Figure 5-6 depicts a simplified view of the traffic flow between multiple clients and a TMG array using an IP affinity–based high-availability solution such as NLB. The funnel represents the virtual-IP (VIP) address used by the high-availability mechanism. The critical point in this scenario is that all traffic—regardless of transport, port, or other criteria—is directed to a specific TMG array member. In this example, TMG 1 receives traffic from client 2, TMG 2 receives traffic from client 3, and TMG 3 receives traffic from client 1.

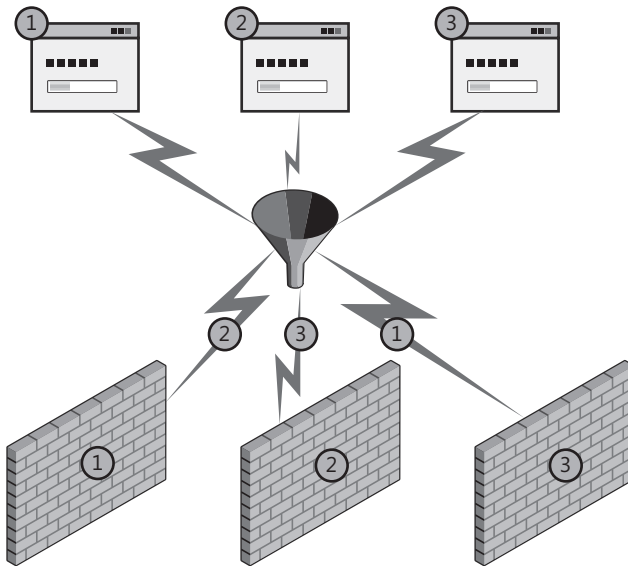


FIGURE 5-6 IP-affinity from multiple sources

NOTE If all three clients were behind a NAT or proxy, they might all appear to come from the same source IP address and would all be directed to the same TMG array member. This is where non-IP-based high-availability may be beneficial.

Figure 5-7 illustrates the typical behavior of a high-availability solution that uses non-IP-affinity, such as source-port or SSL-ID affinity. In this case, the client application opens

multiple connections to the VIP and thus these connections are distributed across the TMG array. If all the TMG array members are publishing the same application server or back-end VIP, this technique may work well. If not, the results could be unpredictable.

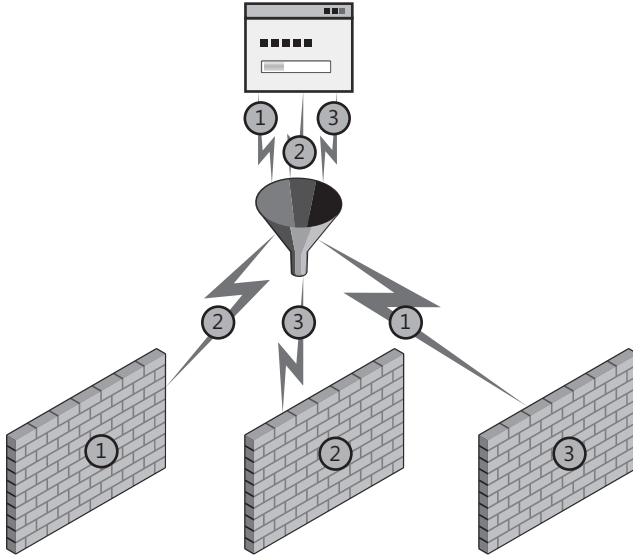


FIGURE 5-7 Non-IP-affinity

NOTE Figure 5-7 illustrates how multiple clients would appear to a high-availability solution if they were isolated by a NAT device or proxy. Because they all use the same source-IP, you must use a non-IP-based affinity method to ensure the best traffic balance across the TMG farm.

Figure 5-8 depicts the behavior of an application that is aware of multiple IP addresses used by a single host. In such cases, the high-availability solution may choose to connect to different destination IP addresses, depending on how the application was designed and tested. This is one reason DNS Round-Robin is not used where predictable client behavior is important. In most cases where the client applications are multi-IP-aware, they will typically use the IP addresses received in the same order they were provided. To provide the best distribution across the TMG array, the order of IP addresses must change in each DNS server response.

At this point you might be asking, “Why didn’t you include the remainder of the 5-tuple in the affinity set?” The answer is that at the server end of the conversation, the destination IP, transport, and destination port is the same for all conversations. Thus, they offer nothing of value to the task of traffic affinity for high availability.

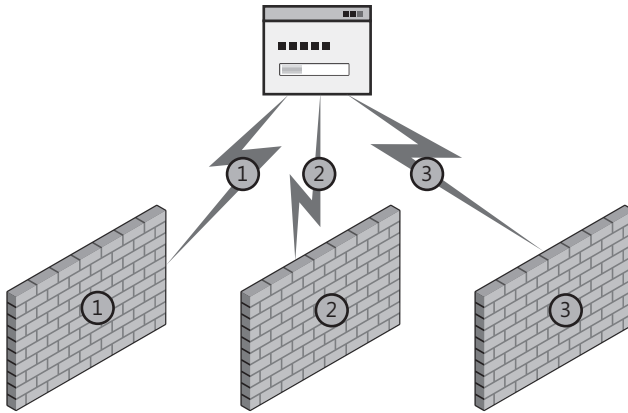


FIGURE 5-8 DNS Round-Robin

In the context of traffic sent through TMG arrays, two basic scenarios impact the high-availability design:

- Traffic handled by publishing rules
- Traffic handled by access rules

In each of these scenarios, you may have the ability to choose between two design options for the TMG network where the client request is seen:

- Integrated NLB
- Third-party solution

We can't address all third-party solutions in this book, but you should be able to use the concepts provided here to compare the functionality and limits of any third-party device you evaluate. Each of the high-availability scenarios also includes the need to evaluate the use of ISP Failover, a new feature introduced in the TMG firewall. We'll examine the considerations for this option in each of the following sections.

Designing High Availability for Publishing Rules

In most cases, publishing scenarios allow TMG to operate as the network service itself as far as the client is concerned. In this scenario, the client communicates with TMG, which then processes, filters, and forwards the traffic to the application server.

Web Publishing

Although typically used to serve requests from the Internet, Web Publishing is also useful for intranet scenarios. The most common use of intranet Web Publishing is to serve Exchange Outlook Web Access (OWA) users. In this scenario, you configure DNS so that connections for the OWA Web site are directed to the TMG Web Listener rather than the Exchange server. You

also configure the Exchange server's OWA listener so that it accepts traffic only from TMG. This allows you to accomplish four goals:

- Provide a consistent login experience for all OWA users.
- Take advantage of customized TMG log on forms.
- Limit the maintenance of the login forms to the TMG.
- Use TMG to protect Exchange from common attacks against OWA.

Intranet Web publishing is also a useful technique to reduce the traffic overhead between branch offices and the central office through the use of TMG HTTP compression and DiffServ traffic prioritization (if your network infrastructure supports it).

On first consideration, Web Publishing appears to impose a fairly well-defined set of constraints for high-availability deployment design. For instance, you only need to consider three protocols for the traffic to the Web Listener; TCP, HTTP, and SSL (TLS). Because the TCP, SSL, and HTTP traffic will always be terminated at the TMG Web Listeners, the traffic is always handled by TMG in a routed context. This is because the traffic operates in the context of "to Local Host," causing the firewall to process the traffic according to Network Rule #1: Local Host Access, which defines this relationship as *route*. Because Network Rules, which define a routed context, are bi-directional, any traffic sourced from TMG to anywhere is also handled in a routed context.

You also need to consider Web Chaining rules for Web Publishing because these are part of any traffic processed by the Web proxy filter. Web Chaining rules are processed after the Web Publishing rule has completed its task. Although Web Chaining rules don't necessarily affect how the high-availability solution for traffic to the Web listener should be designed, they may affect how you design high availability between the TMG array and the published servers.

Because of the way they create and manage connections to the Web application server, some Web applications may not be well suited to some high-availability implementations. To make matters worse, the abuse of the HTTP protocol imposed by some Web applications makes it extremely difficult for many high-availability mechanisms to provide proper handling of this traffic. In particular, Exchange Outlook Anywhere Services and Terminal Service Gateway tend to stretch the HTTP protocol to its limits because of the way RPC is channeled through HTTP.

RPC over HTTP transforms a protocol that was originally designed to handle single-channel simplex traffic into a two-channel, full-duplex transport for each RPC connection between the Outlook client and Exchange server. Because an Outlook client session may incur between 5 and 10 RPC (and thus TCP) connections, this translates to 10 to 20 TCP connections and corresponding HTTP channels for each RPC send/receive context. Unless IP-affinity can be successfully employed, no high-availability current solution can collect all of these connections and sessions into a single context, so these sessions may be split across the TMG array and thus across the Exchange farm as well. Remember that because RPC over HTTP is unable to manage HTTP cookies, we cannot use cookie-affinity to work around this limitation.

MORE INFO *Simplex* refers to a traffic channel where the information flows in one direction. *Duplex* refers to a traffic channel where the information flows in two directions. *Half-duplex* is two-way traffic flow, but in only one direction at a time. *Full-duplex* is also two-way traffic, but both directions can operate simultaneously.

Server (non-Web) Publishing

Because most deployments that use Server Publishing do so against a NAT network relationship, NLB and external high-availability solutions are generally equally effective when compared to their use with Web Publishing scenarios. The biggest difference between Web- and Server-Publishing high-availability solutions is that Server Publishing is typically used for non-HTTP protocols, which effectively eliminates the use of application protocol-specific load balancing techniques such as cookie-based affinity and WPLB.

When Server Publishing is configured in a route relationship, the destination IP address in the traffic sent by the client is the actual IP address of the published server and not TMG itself. Because the destination IP address is not owned by TMG, and because NLB functions only for traffic destined to the local computer, you can't use NLB to provide high availability at the TMG array when the network relationship for a Server Publishing Rule is *route*. In this case, only an external third-party high-availability solution is functional.

ISP Redundancy

Whether you use Web or Server Publishing, the configuration chosen for ISP Redundancy dictates how your publishing rules and the related high-availability solution must operate. ISP redundancy offers two operating modes: ISP failover and ISP load balancing. Both options include two distinct public subnets; the DNS structure that serves the remote clients must be configured according to the ISP Redundancy mode you've chosen so that hosts use the proper route to reach your rule listeners. TMG Integrated NLB and WPLB functionality is effectively unchanged by the ISP Redundancy configuration. Your planning considerations deal strictly with the DNS configuration for each ISP Redundancy option.

When ISP Redundancy is configured for ISP failover, it operates in what is commonly referred to as *active-passive* mode, meaning that only one ISP link is operating at any time. In this mode, your publishing rules may have listeners configured to listen on one or both ISP connections, but only one ISP connection actually processes incoming traffic. Because only one ISP connection accepts traffic at any time, the DNS structure serving those clients must be agile enough to change the responses it provides when the ISP connection changes. The primary concern for this scenario is the time it takes for DNS record changes to be recognized by the rest of the Internet. Contrary to popular belief, DNS records do not "propagate" across the Internet. Instead, each DNS server that holds a copy of the record will query the DNS server that is authoritative for that record (or the nearest forwarding DNS server) for updates to that record. If the Time-To-Live (TTL) for that record is long (for instance, 1 day), it can take

several days for the Internet to realize that this record has changed. This is one reason host TTL is made extremely short for those hosting companies that use DNS Round-Robin for their high-availability or geographic-targeting solution.

When ISP Redundancy is configured for ISP load-balancing, it operates in what is commonly referred to as *active-active* mode, meaning both links are operating at the same time and traffic is shared between them according to the load factor you assigned. In this mode, your publishing rules may have listeners operating on one or both ISP connections. The DNS records relevant to the Forefront TMG listeners determine which listeners receive traffic from remote clients. Figure 5-9 illustrates ISP load-balancing.

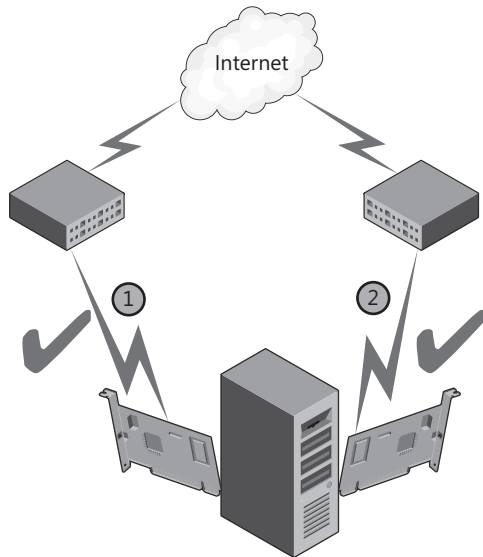


FIGURE 5-9 ISP load-balancing

High Availability from TMG to Published Web Servers

Although the Forefront TMG firewall integrates with NLB to provide an out-of-box high-availability solution for traffic destined to TMG itself, you cannot configure NLB at the TMG server array to provide high availability for traffic that TMG originates. For traffic sourced from TMG itself, other means of high availability are required, such as WPLB, NLB at the published server farm, or third-party solutions deployed between the TMG array and the destination server farm. We'll discuss NLB deployment and configuration in more detail in Chapter 8.

As noted previously, WPLB can use either IP-affinity or HTTP-cookie affinity, but not both simultaneously. Unlike NLB, WPLB does not provide *no-affinity* functionality. The effectiveness of cookie-affinity is completely dependent on the client's ability to process cookies properly. If the client application cannot process cookies properly, WPLB can only be effective if IP-affinity is used. Because WPLB deals with handling traffic to the published applications and

NLB is handling traffic sent to the TMG array, the two are generally compatible when properly configured and all points in the communication (client to TMG to server) can participate properly.

NOTE Because WPLB is provided by a Web filter, and this Web filter is built and configured only for incoming Web requests, WPLB functionality is only available for traffic handled by Web Publishing Rules.

Designing High Availability for Access Rules

When TMG operates as a forward Web proxy for hosts on protected networks, the question of client- versus server-based high availability becomes even more complex, especially when dynamic proxy configuration is employed. Many articles, blogs, and forum postings tout the use of client-side Cache Array Routing Protocol (CARP) as a cheap load-balancing technique, but this is actually much less effective or reliable than DNS Round-Robin and may even create additional problems if you have chosen to use other high-availability techniques for this traffic.

MORE INFO CARP will be discussed in detail in Chapter 16, “Caching Concepts and Configuration.”

External Network

Although it’s not generally a best practice from a security standpoint, many IT administrators will co-locate a server application on the firewall in an effort to save deployment costs. Most often, this sort of deployment is seen in a branch office scenario where cost containment is a higher priority than network security best practices or application isolation. In these cases, Access Rules can be used to allow traffic from remote hosts to the application hosted on TMG. In some cases, Access Rules do not provide the same level of traffic protection as do server- or Web-Publishing rules due to the way TMG application filters process the traffic. Therefore, if you wish to co-locate server applications on TMG, you’re better off if you Web or Server publish the application.

That being said, you configure, maintain, and troubleshoot high availability for access rules on the external network exactly as you would for that high-availability technique when used with Web Publishing and Server Publishing across a NAT relationship.

Protected Networks

Traffic on protected networks offers a very different traffic context for TMG and the connecting clients. As such, your high-availability solutions need to be designed with these facts in mind during the design process.

Hosts communicating through TMG from protected networks use three distinct traffic contexts:

- **SecureNET client** This client is the simplest to design high availability for because it is effectively unaware that the TMG array even exists in the traffic path.
- **Web proxy client** This client is aware that a CERN proxy exists in the network and communicates to it in a specific way.
- **TMG client** This client is aware that TMG exists on the network and uses a complex control protocol set to serve Winsock application requests.

SecureNET clients offer the simplest traffic flow management scenario for the high-availability designer. This client communicates to hosts in remote subnets using its local routing table. One problem you may encounter with this client traffic is that unless you use IP-affinity, each new connection created by this client may be sent to a different member of the TMG array. If the remote server uses source-IP as a security factor (many banking sites do this), and the application creates multiple connections to the remote server, those connections may be seen by the remote server as coming from multiple IP addresses and they all could be disconnected. Needless to say, this behavior can cause your users to apply some creative alternative definitions to the term *high availability*. Some third-party high-availability offerings are smart enough to match the destination IP to existing client connections and thus avoid this problem, but they are not common. NLB does not offer this functionality.

Web proxy clients complicate the high-availability scenario even further because they can operate in one of three ways:

- **Automatic detection** This client configuration uses the WPAD protocol to discover the location of a proxy script. Once the WPAD client acquires the script, this client uses the script to determine how each individual request should be handled.
- **Configuration URL** This client configuration is similar to the automatic detection in that it uses a proxy script acquired from TMG; the primary difference is that it does not use the WPAD protocol to discover the location of this script.
- **Static proxy** This client configuration makes every request to a proxy as specified in the static configuration. Depending on the application, it may make all requests to a specific proxy, or it may communicate with different proxies depending on the protocol in use, such as HTTP, HTTPS (HTTP over SSL/TLS), FTP, and so on. This client configuration does not use a proxy script to determine which proxy to use for individual requests.

IMPORTANT Many Web applications may be configured as any or all of the preceding configurations. In some cases, as with Internet Explorer, Windows Media Player, and many applications based on WinHTTP (Outlook, RDP client, Windows Media, and many others), you can use Group Policy to provide standardized configuration of these applications across all clients in an organization. The Firefox browser even offers an .adm file that allows the Group Policy management of the browser configuration. This template is available from <http://sourceforge.net/projects/firefoxadm/>.

When a Web proxy client uses auto-detection or a configuration URL, the script provided by TMG provides data and code that allows the Web client application to decide whether a destination is local or remote and—if TMG is deployed in a CARP-enabled array—which array member should be contacted to provide the desired content according to the client-side CARP algorithm. What this boils down to is the fact that a Web proxy client application using client-side CARP may make requests to more than one host in the TMG array. Because by default the script lists the array members by IP address, the client-side CARP mechanism should never communicate to a Virtual IP address (VIP) in an NLB-enabled TMG array. In fact, it's best if you don't try to make your high-availability solution work in opposition to the client-side CARP; this creates additional intra-array traffic because the array member that receives the client's request uses the same CARP algorithm to acquire the content from the same server the client tried to contact in the first place. IP-specific load-balancing techniques are a poor choice for these client configurations.

When a client uses a static Web proxy client configuration, IP-specific high-availability solutions tend to work better since each Web proxy application will use the same configuration and so you can direct them to the (VIP) assigned. NLB enabled on the TMG internal network works well for these clients.

TMG clients complicate matters even further, since they acquire a configuration file regardless of whether they are configured for automatic or manual operation. This file tells the TMG client how it should communicate with TMG and which applications require special handling. Because traffic is handled on a per-application basis, it's entirely possible that one application could be operating as a SecureNET client, whereas another is handled as a Web proxy client and still another is handled as a TMG client.

When the TMG client operates with a TMG array, you should use DNS Round-Robin to spread the TMG client load across the array. Each time the TMG client needs to connect to the array, it will ask Windows to resolve the server name, and if the DNS server provides multiple IP addresses for the array FQDN, the TMG client will cycle through those IP addresses for each new application connection. Other high-availability solutions should use IP-affinity to ensure that TMG client traffic does not get split between multiple TMG array members.

ISP Failover

High availability for access rules that serve ISP connections should be handled exactly as you would with Web and Server Publishing across a NAT relationship. For all intents and purposes, they operate exactly the same way.

Joining the Firewall to a Domain or Workgroup

Over the years, administrators have discussed whether ISA Server should operate as domain members. This discussion now applies to the TMG as well. Some conservative, "old guard" firewall administrators think that having a firewall joined to the domain can compromise the

security of the environment. No real proof exists regarding the unsecure state that a firewall domain membership could cause. The good news is that the debate that has been going on and on over the years is becoming less relevant and thus less important.

However, you might still hear statements such as: "If an attacker gains access to the firewall it owns your directory service." This is an untrue statement. No instances of an ISA firewall being compromised in a production environment have been reported, and we expect the same to apply to TMG. Attackers are focused on gaining access to the application services, not gaining access to firewall itself. Table 5-1 outlines the advantages and disadvantages of having TMG operating in the domain or workgroup.

TABLE 5-1 Domain vs. Workgroup

FOREFRONT TMG INSTALLATION	PROS	CONS
Domain-Joined	<ul style="list-style-type: none">■ More granular control for user access in forward and reverse proxy scenario.■ Full support for client certificate authentication as the primary authentication method.■ No need to have a certificate for connectivity with CSS.■ Support for Active Directory Group Policy. This can add another layer of protection when hardening the TMG computer by using Group Policy.■ Enhanced security while publishing services, such as Exchange Server by using Kerberos Constrained Delegation.	<ul style="list-style-type: none">■ If your TMG Server is located in a Perimeter network in front of another firewall, you need to allow more protocols through it to allow communication with the domain.
Workgroup	<ul style="list-style-type: none">■ If the firewall is compromised, the directory services might not be affected.	<ul style="list-style-type: none">■ Requires additional overhead for administration because a certificate is required if CSS is installed in Workgroup.

FOREFRONT TMG INSTALLATION	PROS	CONS
	<ul style="list-style-type: none"> ■ Even if Active Directory is compromised, the firewall might not be compromised because it isn't part of the domain. 	<ul style="list-style-type: none"> ■ Doesn't have the same flexibility to use domain users and groups for outbound access. ■ Can't use client certificates as the primary authentication method. ■ User accounts are created on the firewall itself to allow intra-server communication. ■ Doesn't support Active Directory Group Policy. ■ TMG client authentication requires account mirroring on TMG

Although this table gives you a set of comparative parameters, in some scenarios you will see TMG implemented in a workgroup. Most of the time this happens because of one of the following reasons:

- A lack of information about the real benefits of having the TMG as a domain member
- A back-to-back firewall scenario where TMG (firewall and CSS) is placed between two third-party firewalls and the firewall administrator wants to avoid opening RPC and other port from Forefront TMG to the internal network
- A company security policy that determines that no device that faces an untrusted network can be part of the corporate domain

Among the preceding arguments, the most understandable one from a political and sociological perspective is the last one, because it involves something that usually comes from management and is not based on technical facts. You can work around the other two arguments if the security administrator has a good understanding of the benefits of deploying the TMG as a domain member.

Summary

When you plan your TMG deployment, you have two choices: Design the network around the TMG deployment or fit TMG into an existing network structure. Because the highest probability is that TMG will have to fit an existing structure, you've most likely already had the opportunity to think through the requirements of your network and high-availability needs and match your TMG deployment to them. Now that you know the elements that you need to address prior to choosing your network template, you can start planning your migration. In the next chapter you will learn how to migrate from ISA Server 2004 or ISA Server 2006 to TMG.

Using Network Monitor 3 for Troubleshooting TMG

- Using Network Monitor to Capture Traffic **891**
- Reading a Network Monitor Capture **897**
- Troubleshooting TMG Using Network Monitor **903**
- Summary **909**

Microsoft Forefront TMG includes some built-in tools to assist in troubleshooting various scenarios, such as publishing rules and access rules. However, in some situations you will need to go a step further and analyze what is happening on the wire to better understand TMG behavior. For those scenarios the best tool to use is Network Monitor. This chapter will cover the basics of Network Monitor, including how to capture data and some Network Monitor capture scenarios.

Using Network Monitor to Capture Traffic

As explained in Chapter 4, “Analyzing Network Requirements,” the definition and understanding of your network’s traffic profile is important so that you can know precisely what TMG should handle as far as protocols are concerned. Perhaps you have proprietary applications that are not using default ports and therefore you need to create a custom protocol definition on the TMG firewall. Commonly, in medium and large network environments not all applications used on the client workstation are precisely documented—the protocol and port the workstation uses are not always described.

MORE INFO The following blog post offers an example of how Network Monitor can assist you in identifying unknown traffic: <http://blogs.technet.com/yuridiogenes/archive/2008/10/19/using-Network-Monitor-3-2-to-identify-an-unexpected-traffic.aspx>.

Sometimes applications are deployed to client workstations without proper documentation and without you understanding how the application works. These scenarios gain complexity when the application needs to use a server located outside of the internal network and the traffic needs to pass through TMG. Without proper documentation from the application vendor, you will have to investigate what protocols the application requires to create access rules on TMG firewall.

This is only one example of a scenario in which you can use Network Monitor to identify traffic patterns and troubleshoot network connectivity issues. The version that we use in this book is the currently available public version (at least at the time of this writing), which is Network Monitor 3.3.

MORE INFO Watch for new releases and for articles related to Network Monitor at the Network Monitor Team's blog: <http://blogs.technet.com/netmon>.

Data Gathering with Network Monitor

When using Network Monitor for data gathering it is important to define your primary goal. In other words, what are you looking for? Many times a Network Monitor capture becomes painful to read because whoever is reading it doesn't know what to look for. When you have a clear understanding of the goal of this capture, you can move forward to the next step, which is configuring Network Monitor for data gathering.

Network Monitor allows you to capture data using the Network Monitor Graphical User Interface (GUI) or by using the *nmcap* command-line interface. Troubleshooting scenarios with TMG sometimes require Network Monitor capture plus other logs. This is the nice thing about ISA Data Packager (which is part of the ISABPA): this tool also gathers Network Monitor captures from all TMG firewall network interfaces.

MORE INFO See the following post for more information on ISA Data Packager: <http://blogs.technet.com/yuridiogenes/archive/2009/05/07/using-isabpa-for-proactive-and-reactive-work-with-isa-server-part-2-of-2.aspx>.

Using Network Monitor GUI

When performing a capture using the Network Monitor console, you need to address some issues before you get started. Figure 33-1 shows the Network Monitor interface, highlighting the main features available.

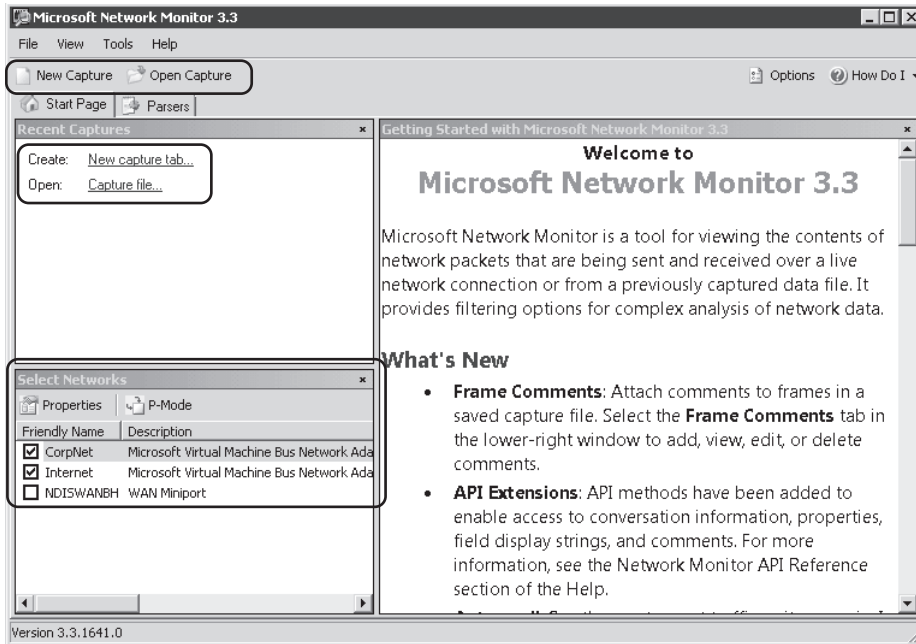


FIGURE 33-1 Network Monitor main screen

By default Network Monitor gathers data only on the following scenarios:

- Traffic generated from the interface that you selected
- Traffic where the selected interface is the destination
- Broadcast traffic

If you want to gather all traffic seen by this interface—including that which has nothing to do with this interface—you need to click the P-Mode (Promiscuous Mode) button on the Select Networks panel. The Select Networks panel also presents the available network interfaces; this is one of the most important options in this dialog box. The majority of the issues that you troubleshoot on TMG will require you to get a Network Monitor capture for all relevant network interfaces on the TMG computer. To do that you need to clear the checkbox for any interfaces (by default both will appear selected) on which you do not wish to capture data and then click the New Capture tab (either on the toolbar or on the Recent Captures panel).

When a new Capture tab is created you will see a dialog box similar to the one shown in Figure 33-2.

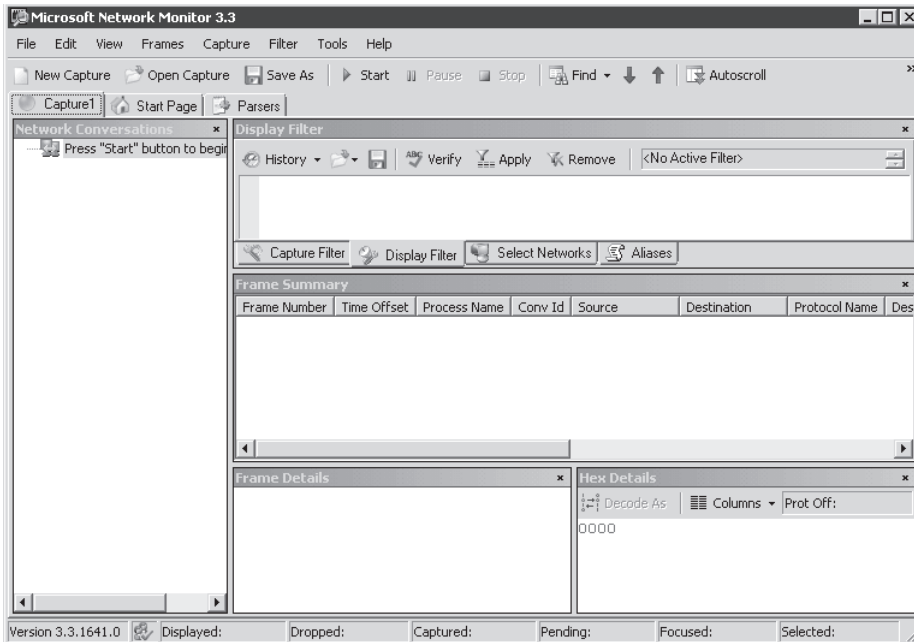


FIGURE 33-2 New capture dialog box and the initial options for data gathering

When you are ready to reproduce the issue that you are troubleshooting, click the Start button located in the toolbar, as shown in Figure 33-2. When Network Monitor captures the traffic it creates a file to temporarily store the captured data. This file has a predefined size determined in the Network Monitor Options dialog box, and after it gets full, Network Monitor starts to overwrite the older packets capture within the capture's temp file. To change the temp file location and the buffer size follow these steps:

1. Click Tools.
2. Click Options.
3. Click the Capture tab. The dialog box shown in Figure 33-3 appears.
4. Change the file location and the buffer size and then click OK.

After you finish reproducing the problem, click the Stop button to stop the capture and save the file by using the option Save As from the File menu. The Save As dialog box appears, as shown in Figure 33-4.

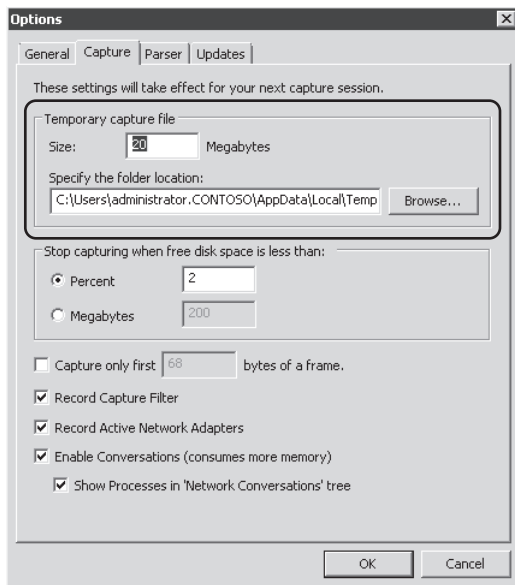


FIGURE 33-3 Available options for temp file location and buffer size

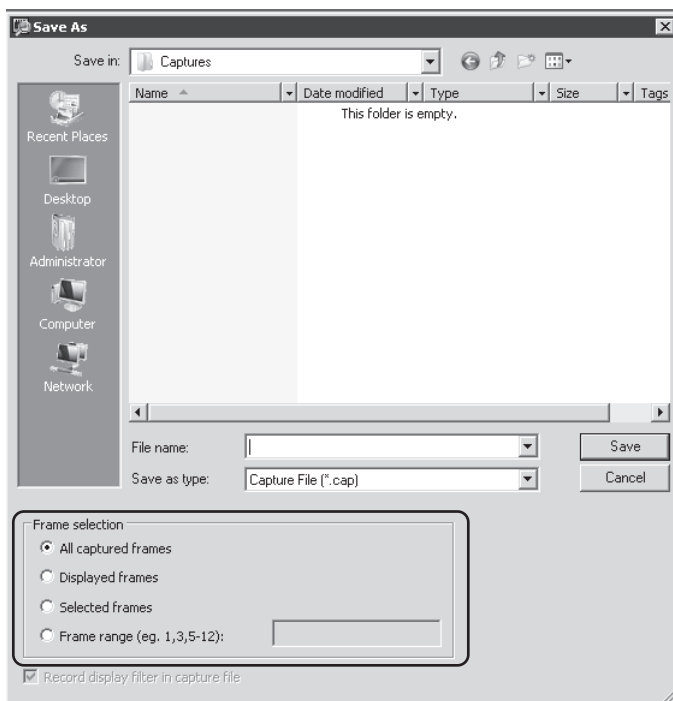


FIGURE 33-4 Selecting which frames you want to save

The following frame selection options are available in the Save As dialog box:

- **All Captured Frames** Saves all the frames that were captured. Save the temp file with the name that you choose and then delete the temp file.
- **Displayed Frames** Saves only the frames that are displayed in the capture tab. This option can be interesting if, for example, you want to save only the HTTP traffic from TMG to a specific IP address. You can create and apply a filter and you will only see frames that belong to this filter. This will reduce the final size of the .cap file that you are saving.
- **Selected Frames** Saves only the frames that you selected (highlighted) in the capture dialog box.
- **Frame Range (e.g., 1,3,5-12)** Saves only a specific range of frames.

NOTE Later in this chapter we will explain how to analyze a capture and use the available options within the Capture tab in the Network Monitor interface.

Using Nmcap.exe

The user experience with Network Monitor GUI is much better than Network Monitor 2 for most scenarios. However, in some other scenarios automation and system resource usage are more important than having a nice interface in which to capture and interpret data. To limit the resources consumed by Network Monitor during the capture process, you can use the *Nmcap* command-line interface, which has a rich set of options for data gathering. For the purpose of this example you will capture traffic from all interfaces where the protocol is equal to HTTP (*/capture http*), setting a maximum file size to 40 MB (*/file httptraffic.cap:40M*) and stopping when you press the X key (*/terminatewhen /keypress x*). To accomplish this access follow these steps:

1. Click Start, type **cmd**, and press Enter.
2. Type following the command:
`Nmcap /network * /capture http /file httptraffic.cap:40M /terminatewhen /keypress x`
3. Press Enter. Open Internet Explorer and browse to *http://www.microsoft.com*. After navigating through the site, go back to the command prompt window and press the X key.
4. A file called httptraffic.cap will be available in the location where you started this command, which is the Network Monitor folder.

To see all the parameters available in the *Nmcap* command-line interface, type the command **nmcap /?**. To see some example scenarios of how to use *Nmcap*, type the command **nmcap /example** and press Enter.

NOTE A tool called the Network Monitor Wizard was created to assist in the task of configuring the *Nmcap* command-line based on parameters that can be specified by stepping through the wizard. You can download this tool (and the source code) from <http://netwiz.codeplex.com>.



REAL WORLD The Infamous 5783 Event

One of the most challenging scenarios for data gathering is the one that happens intermittently, where there is no immediately discernable pattern and when there is no one available to get data. A classic example is when the ISA or TMG firewall loses connectivity with a domain controller and triggers the event 5783 in the System Log, which says that no domain controllers are available. This problem can be caused by so many issues that a broad data gathering method is required to really understand what is going on.

Nmcap does not have a way to stop a capture if a particular event happens. However, one option you can use in the Windows Server 2008 Event Viewer feature allows you to trigger an action when a specific event occurs. However, this is not an ideal option because when event 5783 appears, it means that the issue already happened—the communication of interest is done, and capturing data from this point will not reveal what happened during that precise time frame. In a scenario like this the goal is really to keep capturing *until* the event happens. In other words, stop Network Monitor capture when event 5783 appears in the event log.

Fortunately, the Network Monitor Team listens to the user community and has developed a helpful tool called NM3EventCap. For this particular case the command line is pretty simple. Just type **NM3EventCap.exe TheEvent.cap 5783**. You can use other parameters, such as the maximum file size, number of adapters to capture, and so on. Download this tool from <http://nm3eventcap.codeplex.com>. This tool was built based on Network Monitor API, which you can also start playing with by downloading the SDK from <http://nmexperts.codeplex.com>.

Reading a Network Monitor Capture

Analyzing network captures is an exercise made up of 50 percent knowledge and 50 percent experience. A dazzling number of digital and print references are available that are intended to help you improve your network analysis skills. Network capture analysis requires at least a basic knowledge of the behavior expected from the application under test as well as some familiarity with the related protocols. The time spent using multiple capture and analysis tools will help you gain these skills.

NOTE Laura Chappell of <http://www.wiresharku.com> offers a vast array of network analysis training. Although the content is Wireshark-focused, the concepts and techniques transfer quite well to Network Monitor. She has presented sessions on network analysis techniques at numerous venues such as Tech Ed and Black Hat.

If you've never used a network analysis tool, you need to understand a few things about how Network Monitor processes network captures:

- All network traffic is divided into data chunks called *packets*.
- The packets contain data relative to one or more protocols.
- The protocols in these packets are identified and analyzed using protocol parsers.
- One parser can call another parser if it has been written to recognize the protocol handled by the next protocol layer parser.

When you open a network capture file, Network Monitor passes the file data through its parser engine, which in turn calls the related protocol parsers as each protocol is identified. The result of this action is displayed to you in the Frame Summary pane of the Network Monitor application window, as shown in Figure 33-5.

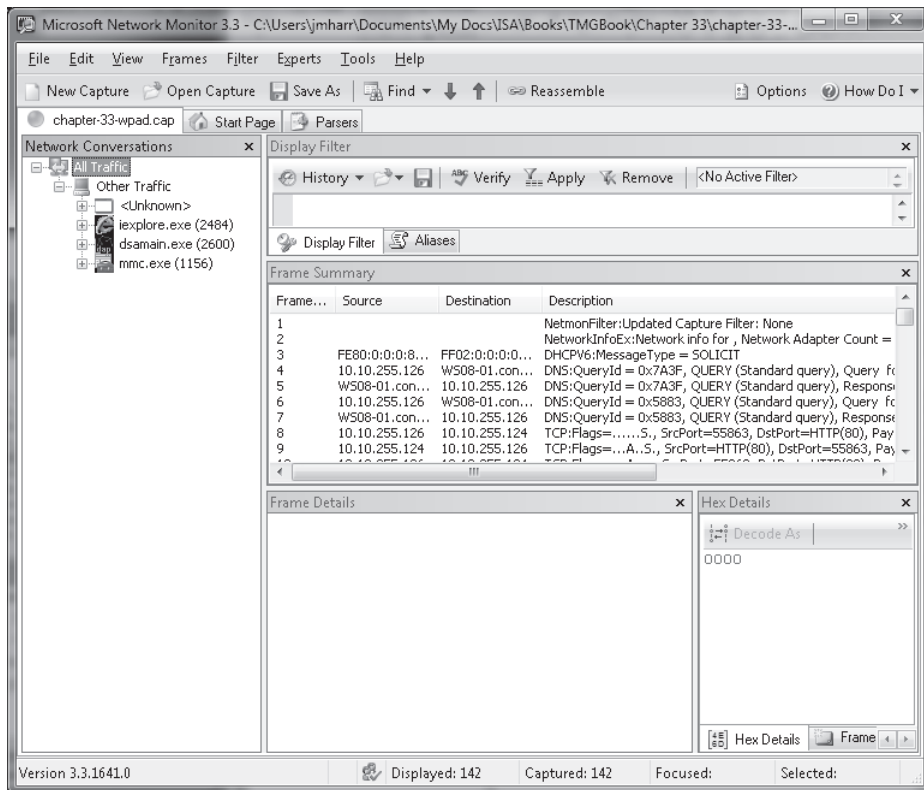


FIGURE 33-5 Network Monitor display example

In the left pane, Network Monitor displays a summary of the IP conversations identified by the parsers that were called by the Network Monitor parsing engine. By default, Network Monitor limits this display to the lowest-layer protocol; in this case, the application process name and process ID are shown because the capture was taken with these options enabled.

Each conversation is assigned a unique number to help you filter the capture so that only the protocols you are interested in are displayed.

You can click the plus sign (+) indicator to expand an IP conversation to display the higher-layer protocols, each of which can be expanded if it contains a higher-layer protocol. If you select one of the conversations in the left pane, the Frame Summary pane is updated to show only those packets that are related to that protocol and conversation. Figure 33-6 illustrates this relationship for one of the conversations.

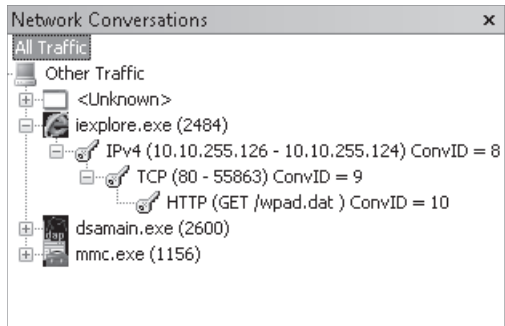


FIGURE 33-6 Conversation summary display

If the data is saved as part of the capture file, Network Monitor organizes the conversation summary so that the relationship between applications and the protocols is clear. If the process information is not part of the capture, Network Monitor only shows the protocol relationships. In the example shown in Figure 33-6, HTTP conversation 10 is part of TCP conversation 9, which in turn is related to IP conversation 8 and was created by iexplore.exe (Internet Explorer) process ID 2484. One thing to remember about Network Monitor conversation identifiers is that they are assigned as each parser tells the parser engine to create a conversation. Because higher-layer protocols are called by lower-layer protocols, the conversation value represents the total number of conversations Network Monitor has identified up to that point in the capture, not the conversation count for a particular protocol. In other words, HTTP conversation 10 represents the tenth conversation Network Monitor was instructed to build, not the tenth HTTP conversation Network Monitor identified.

These values are useful in the display filter pane as values provided in the Conversation. *Protocol.ID*, where *Protocol* is replaced by the name of the protocol of interest, such as TCP, HTTP, and so on. If you wanted to limit the display to HTTP conversation 10, you would type **conversation.http.id=10** in the Display Filter text box and click Apply or press Ctrl+Enter to apply the filter.

Network Monitor also provides the means to filter the capture on any *parsed* aspect of the capture data. Network Monitor depends on the protocol parsers to help with this functionality because it is the parser's responsibility to interpret the data and identify key aspects of the protocol that can be used by you in your analysis efforts. For instance, if you want to limit the display to TCP traffic to and from the TMG Web Proxy listener for a protected network, but you don't yet know the conversation, you can use the display filter

statement **tcp.port==8080**. Network Monitor allows you to apply the port number to the source and destination ports simultaneously by using the generic *.port* property. By using this generalization for source and destination ports, the display will show traffic to and from TMG, not just to TMG (as with `tcp.dstport==8080`) or traffic from the TMG Web Proxy listener (as with `tcp.srcport==8080`). This applies to UDP as well as TCP because they both utilize source and destination ports as part of the protocol.

This is where having a basic understanding of most common protocols is useful. If you try to apply a display filter to a protocol that doesn't define a property you specify in the display filter, or if you specify an invalid value, Network Monitor will indicate an error and the current Frame Summary display will be unchanged. Figure 33-7 illustrates this behavior.

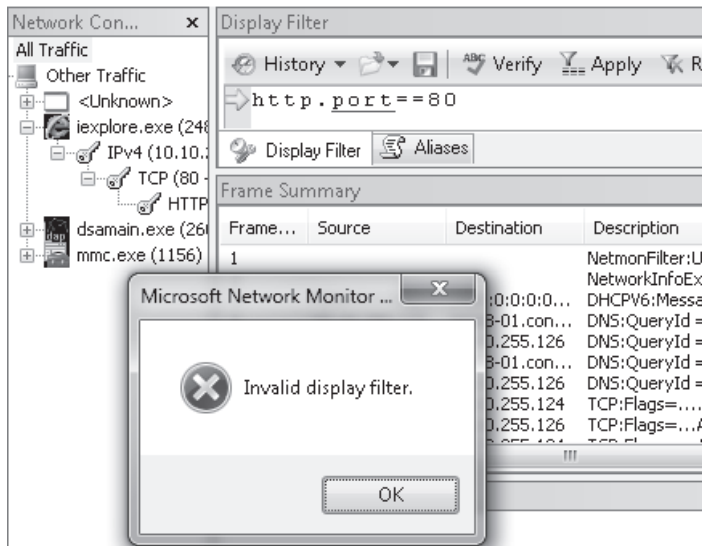


FIGURE 33-7 Network Monitor invalid filter response

The example in Figure 33-7 illustrates a common misunderstanding of protocol relationships. It's generally accepted in the networking community that TCP port 80 is used for HTTP, but a common misunderstanding is that port 80 is part of the HTTP protocol itself.

Recall from Chapter 15, "Web Proxy Auto Discovery for TMG," that the WPAD process is actually made up of three separate protocols:

- DHCP to discover the WPAD URL
- DNS to discover the WPAD host record or resolve the name obtained in the DHCP INFORM response
- HTTP to request the CFILE (configuration file)

If you want to isolate the traffic related to WPAD, you have to use a more complex display filter statement than just ports. There is no way to write a single filter called WPAD, but because you know which protocols are involved, you can write a display filter that includes only the protocols that are part of the WPAD process. The simplest filter would appear as

dhcp or dns or http, instructing Network Monitor to display only the packets that include those three protocols. Unfortunately, it would also display the DNS, DHCP, and HTTP traffic that was not related to WPAD.

You can create a filter that limits the traffic to only the data you want, but it takes a bit of sleuthing to gather the data you need to provide to Network Monitor. Because the Network Monitor team is owned and operated by some very experienced networking folks, they understand the need to make this task as simple as possible. The following steps illustrate how to use Network Monitor to build the query needed to isolate only WPAD-related traffic. The capture file is included on the companion CD as chapter-33-wpad.cap. The example capture doesn't include DHCP traffic, so you get to limit your efforts to DNS and HTTP only.

NOTE To open the example captures, you have to install Network Monitor on your computer. You can obtain the latest version from <http://www.microsoft.com/downloads/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f> and the latest parsers can be obtained from <http://www.codeplex.com/NMParasers>.

Open Network Monitor

1. Click Start and then click All Programs.
2. Expand Microsoft Network Monitor 3.3 and then click Microsoft Network Monitor 3.3.

Open the Example Capture File

1. In Network Monitor, click Open Capture and navigate to your CD drive.
2. Select chapter-33-wpad.cap and click Open.

Apply the Basic WPAD Display Filter

1. In the Display filter text box, type **dns or http**.
2. Click Apply or press Ctrl+Enter to apply the filter to the Frame Summary display pane.

Your Network Monitor display should appear, as shown in Figure 33-8.

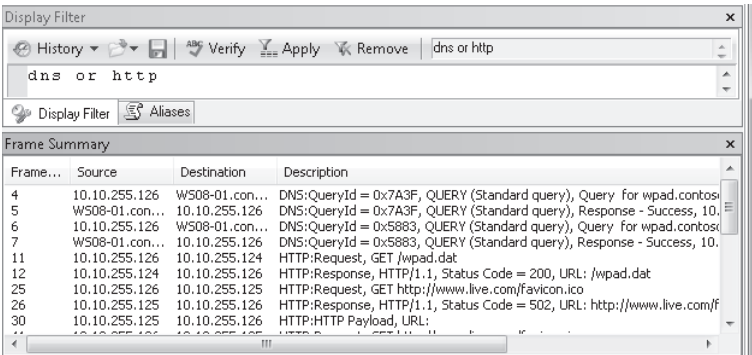


FIGURE 33-8 Initial Frame Summary display

Narrow the DNS Filter Scope

1. In the Frame Summary pane, select Frame 6 (DNS Query for wpad.contoso.com). This is the DNS query for the WPAD record. The Frame Details pane will display the protocol details for this packet.
2. Starting with the DNS protocol in the Frame Details pane, expand each following item until you see QuestionName: wpad.contoso.com.
3. Right-click QuestionName: wpad.contoso.com and select Add Selected Value To Display Filter. The Display Filter text box will change to "dns or http OR DNS.QRecord.QuestionName == "wpad.contoso.com"".

Narrow the HTTP Filter Scope

1. In the Frame Summary pane, select Frame 11. This packet is the WPAD request from the client to TMG. The Frame Details pane will display the protocol details for this packet.
2. In the Frame Details pane, expand the data points within HTTP until you see the host: wpad.contoso.com.
3. Right-click host: wpad.contoso.com and select Add Selected Value To Display Filter. The Display Filter text box will change to "dns or http OR DNS.QRecord.QuestionName == "wpad.contoso.com" OR HTTP.Request.HeaderFields.Host == "wpad.contoso.com"".
4. In the Frame Summary pane, select Frame 12. This packet is the WPAD response from TMG to the client. The Frame Details pane will display the protocol details for this packet.
5. In the Frame Details pane, expand the data points within HTTP until you see MediaType: application/x-ns-proxy-autoconfig.
6. Right-click MediaType: application/x-ns-proxy-autoconfig and select Add Selected Value To Display Filter. The Display Filter text box will change to "dns or http OR DNS.QRecord.QuestionName == "wpad.contoso.com" OR HTTP.Request.HeaderFields.Host == "wpad.contoso.com" OR HTTP.Response.HeaderFields.ContentType.MediaType == "application/x-ns-proxy-autoconfig"."

Narrow the Whole Display Filter

1. In the Display Filter pane, delete "dns or http OR" from the display filter text. The remaining text should read "DNS.QRecord.QuestionName == "wpad.contoso.com" OR HTTP.Request.HeaderFields.Host == "wpad.contoso.com" OR HTTP.Response.HeaderFields.ContentType.MediaType == "application/x-ns-proxy-autoconfig"."
2. In the Display Filter pane, click Apply or press Ctrl+Enter to apply the display filter. The Frame Summary pane contents should resemble Figure 33-9.

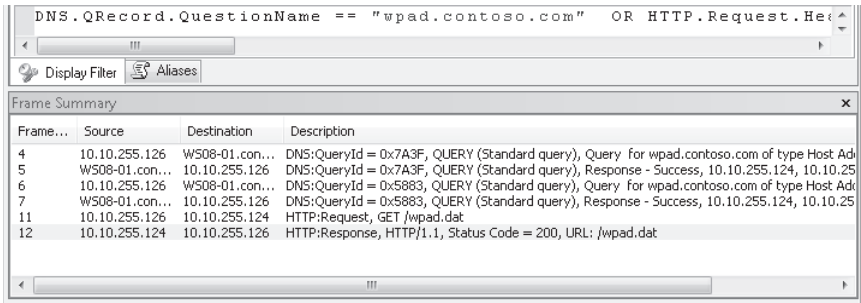


FIGURE 33-9 WPAD display filter results

Congratulations! You've just defined a filter that will specifically identify the DNS and HTTP portions of the WPAD process used by any host in the Contoso organization. Because Network Monitor also allows you to save filter definitions, you need never be forced to re-create this little gem.

NOTE If you wanted to further isolate the search in a very large capture to a single client, you need only add that client IP address to the filter definition. If the client in question were operating on IP address 192.168.0.123, that filter would appear as "ipv4.address==192.168.0.123 and (DNS.QRecord.QuestionName == "wpad.contoso.com" OR HTTP.Request.HeaderFields.Host == "wpad.contoso.com" OR HTTP.Response.HeaderFields.ContentType.MediaType == "application/x-ns-proxy-autoconfig")". You need to add the parentheses around the original filter definition so that all of the original filter criteria apply equally to the IP address.

Troubleshooting TMG Using Network Monitor

In this part of the chapter, you'll see how to use various Network Monitor display filters to help evaluate a SOCKS-proxy application's misbehavior. The capture used in this example is contained on the companion CD as socks4_ftp.cap.

In this scenario, a colleague has decided that he wants to test how Internet Explorer (IE) behaves as a SOCKS proxy client when accessing FTP servers. He believes the TMG and IE configurations are correct, but he has two problems that he needs your help to resolve:

1. His internal DNS structure does not allow clients to resolve public names to IP addresses, yet IE is able to make the connection to the FTP server.
2. Although IE is apparently able to connect to the FTP server, IE cannot display a directory listing from the FTP server.

At your request, he obtained a Network Monitor capture at the test client during an attempt to use the ftp.3com.com FTP server and sent it to you for analysis. When you open the capture file, Network Monitor initially displays an unfiltered protocol analysis as shown in Figure 33-10.

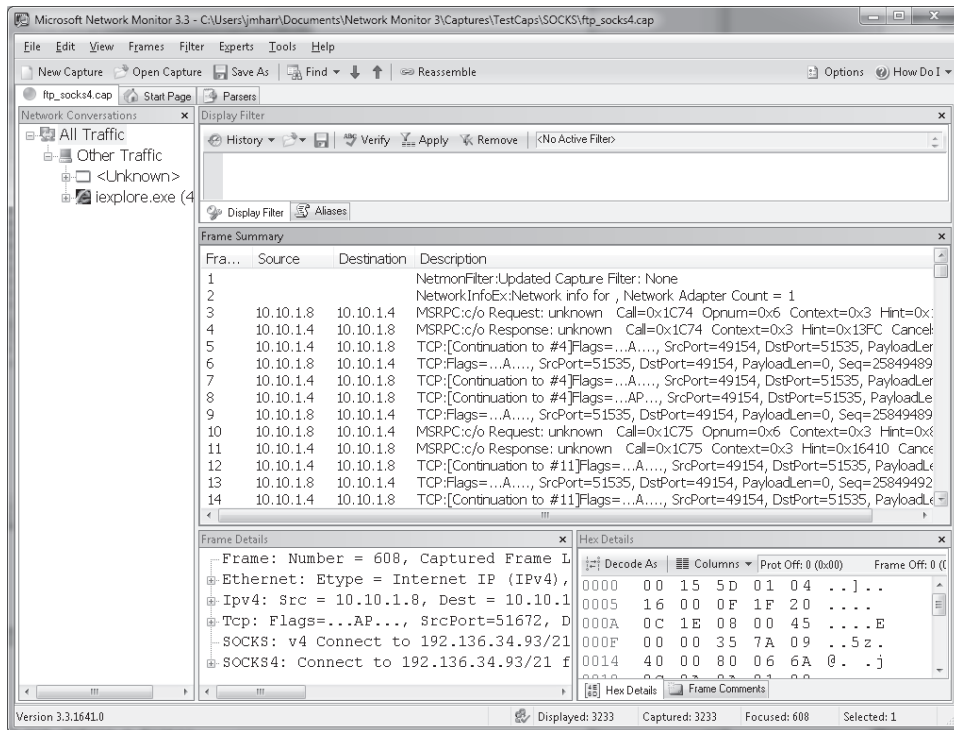


FIGURE 33-10 Initial Network Monitor display for socks4 FTP capture

You'll notice that because your colleague did not define a filter during the capture, it contains a lot of traffic that appears to be unrelated to the issue you're evaluating—at least right now. You'll see the value of an unfiltered capture as we move through the analysis.

Because you know that your colleague is testing the browser as a SOCKS client, you can apply a display filter to limit the traffic Network Monitor displays to that protocol. You do this by performing the following steps:

1. Enter the name of the protocol (SOCKS) in the Display Filter pane just above the Frame Summary pane, as shown in Figure 33-11.
2. Either click Apply in the Display Filter pane or press Ctrl+Enter to apply the filter to the Frame Summary display.

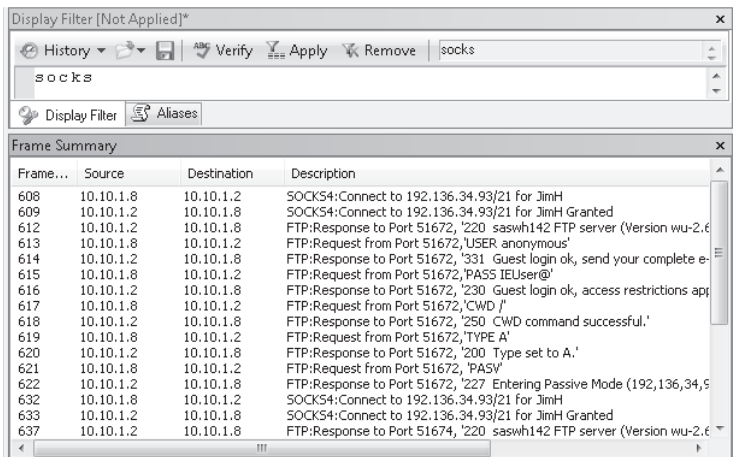


FIGURE 33-11 Frame Summary display filtered for SOCKS protocol

Initially, the capture seems to indicate behavior that is typical of an FTP application configured as a SOCKS proxy client:

1. IE sends a SOCKS CONNECT for IP address 192.136.34.93 and port 21 (FTP control channel). Because IE specified the IP address instead of the FTP server host name, it's clear that IE is indeed resolving the host name to the IP address.
2. The SOCKS proxy replies with GRANTED. This response demonstrates two facts:
 - a. The SOCKS proxy rules allow this request.
 - b. The connection to the requested destination was successful.
3. Immediately following the SOCKS GRANTED reply, you see the FTP banner in Frame 612. This tells you that the FTP server is functioning at a basic level.
4. The FTP server accepts an anonymous login from IE. You can determine that whatever problem your colleague is having, it's not related to FTP server authentication.
5. The FTP server accepts the IE instruction to change the working directory to the root directory (CWD /).
6. The FTP server accepts the IE command to send ASCII data (TYPE A).
7. The FTP server accepts the PASV command sent by IE and responds with the IP and port that the FTP server has prepared for IE to connect to for use as the FTP data channel. In this case, IE should connect to the FTP server on IP address 192.136.34.93, port 43799.

NOTE FTP commands that describe listeners using addresses and ports are expressed using six-value, comma-separated decimal values. The IP address occupies the first four values and the port is described by the fifth and sixth values. The two port values combine to represent the two bytes of a 16-bit value. The first byte-value is the "high byte" and so represents a multiplier of 256. In this case, the high-byte value is 171,

which produces a literal value of 43776. The second value is 23, which is added to the high byte to produce the actual port: 43799. The FTP response “227 Entering Passive Mode (192,136,34,93,171,23)” literally means “I’m expecting a connection from you on IP address 192.136.34.93, port 43799.”

8. IE then issues a SOCKS CONNECT command for IP address 192.136.34.93 and port 21 (FTP control channel).

The process indicated in steps 5 and 6 is typical of an FTP client that is preparing to send a Print Working Directory (PWD) command to an FTP server (similar to the Windows DIR command). What is unusual about this capture is that immediately after the FTP server tells IE how it should establish the FTP data channel connection, IE issues the SOCKS CONNECT request for the *same destination and port as the FTP control channel*. Clearly, this is not what IE should be doing at this point. Because we don’t have visibility into the logic IE is using, we have to proceed using reasonable assumptions.

One thing that may have happened is that IE determined that it was unable to establish the FTP data channel connection as directed by the FTP server and decided instead to restart the whole process with the FTP server. Because the capture does not indicate that IE tried to make a SOCKS connection to the FTP server data channel listener, we can see whether IE tried to make a direct connection. To determine whether this is the case, change the display filter to limit the output to the FTP server IP address by following these steps:

1. Type **ipv4.address==192.136.34.93** in the Display Filter pane just above the Frame Summary pane, as shown in Figure 33-12.

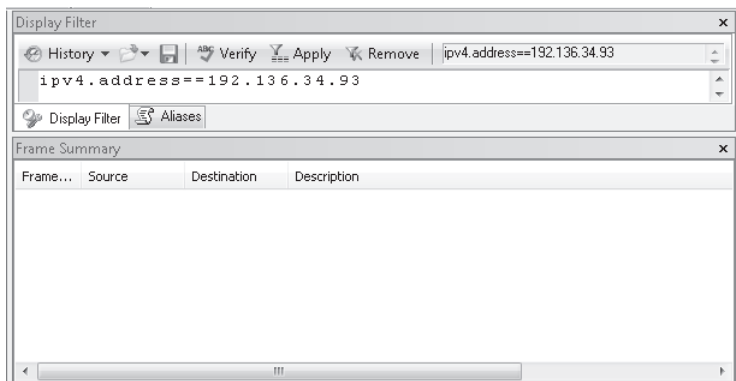


FIGURE 33-12 Frame Summary filtered for FTP server IP address

2. Either click Apply in the Display Filter pane or press Ctrl+Enter to apply the filter to the Frame Summary display.

It seems clear from the Frame Summary display in Figure 33-12 that IE did not try to make a direct connection to the FTP server for the data channel connection. Although this clarifies the scenario for you, it does raise some questions about IE behavior as a SOCKS proxy client.

Now that you can demonstrate why your colleague cannot obtain a directory listing from the FTP server and have the isolated the data required to prove it, you decide to move to the question of name resolution for public names that shouldn't work.

A network capture can't tell you *why* IE is choosing to establish another FTP control channel when it should be establishing an FTP data channel using the parameters provided by the FTP server, but the capture does provide the empirical data your colleague will need when he calls Microsoft Customer Support Services (CSS).

To answer the question of name resolution, your next step would be to filter the capture on the DNS protocol by following these steps:

1. Enter the name of the protocol (DNS in this case) in the Display Filter pane just above the Frame Summary pane, as shown in Figure 33-13.

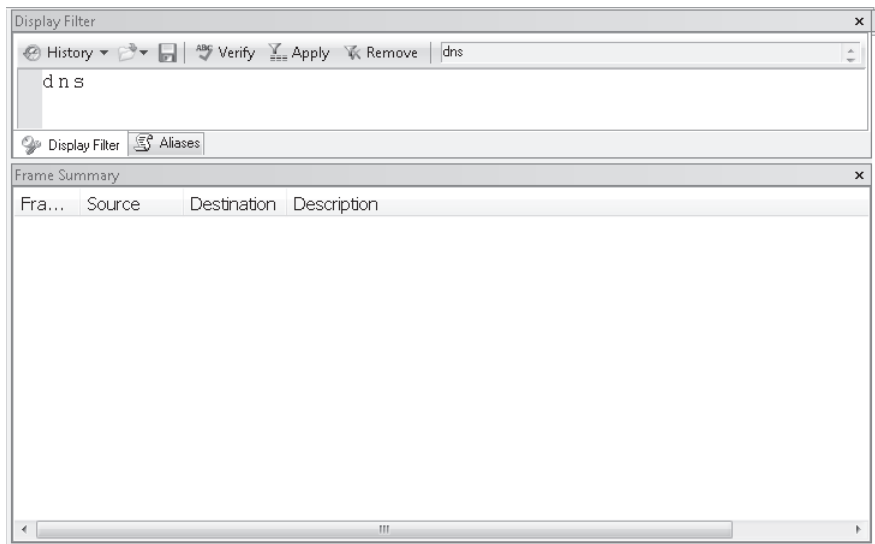


FIGURE 33-13 Frame Summary display filtered for DNS

2. Either click Apply in the Display Filter pane or press Ctrl+Enter to apply the filter to the Frame Summary display.

It seems clear that the client did not issue any DNS queries at all—much less for ftp.3com.com, so the question now is how was IE able to resolve the name “ftp.3com.com” to an IP address?

One thing Network Monitor can do that no other network traffic capture tool does is to include the application process that is generating or accepting network traffic. This provides you with the ability to filter the traffic based on the process that Windows associates with the traffic. Although this is only possible if the capture was taken using Network Monitor 3 or later on a Windows computer, it is nonetheless a very valuable feature, as you'll soon see.

Network Monitor builds the application-to-traffic association in the context of a conversation. To see all the traffic Network Monitor associated with IE while your colleague was taking the capture, follow these steps:

1. Type **Conversation.ProcessName.contains("iexplore")** in the Display Filter pane just above the Frame Summary pane, as shown in Figure 33-14.

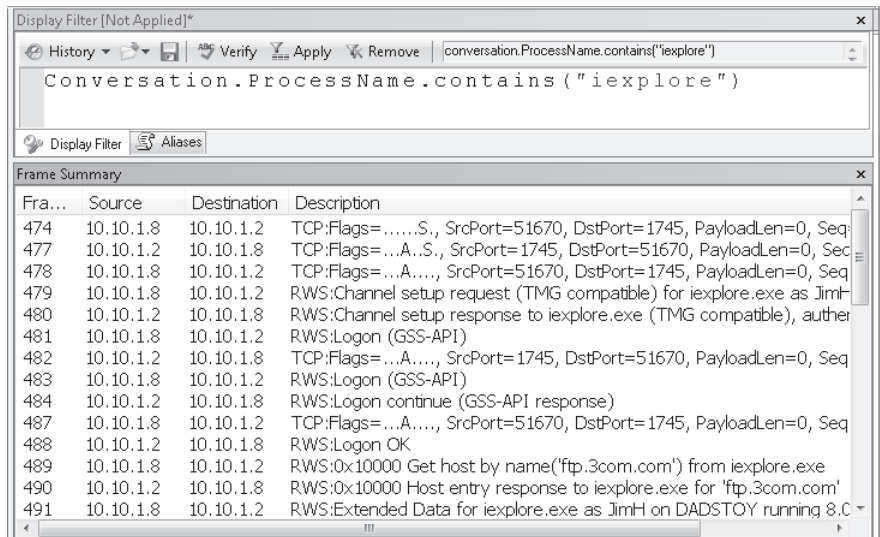


FIGURE 33-14 Frame Summary display filtered for DNS

2. Either click Apply in the Display Filter pane or press Ctrl+Enter to apply the filter to the Frame Summary display.

The first thing you notice is that Network Monitor is displaying a protocol named RWS that includes a reference to TMG. The RWS protocol is one of two protocols used by the TMG Client (TMGC) to communicate with TMG. Therefore, you may surmise that your colleague has the TMGC installed on his test computer.

MORE INFO You can start your TMGC protocol education on TechNet at <http://technet.microsoft.com/en-us/library/ee291341.aspx>.

As you examine the conversation between the TMGC and TMG, you notice that among other things, the TMGC sends a "Get host by name('ftp.3com.com') from iexplore.exe" message to TMG, which responds with a "Host entry response to iexplore.exe for 'ftp.3com.com'" message to the TMGC. Because you learned from the TechNet article that "Get host by name" is related to name resolution, you decide that this part of the conversation merits deeper investigation. You can examine the host entry message in greater detail by selecting the packet in the Frame Summary pane. When you do this, the packet details are displayed in the Frame Details pane. You can view more detail of each protocol by clicking the plus

sign on the left side of the display to expand that item. You can continue this process until you find the data that you are seeking. In this case, although you are reasonably sure that IE is resolving the name ftp.3com.com to an IP address via TMG, you want to prove this theory conclusively. You do this by expanding each node in the RWS protocol as it is displayed until you locate the IP address IE used in the SOCKS CONNECT command. Figure 33-15 shows the part of the RWS message that includes this data.

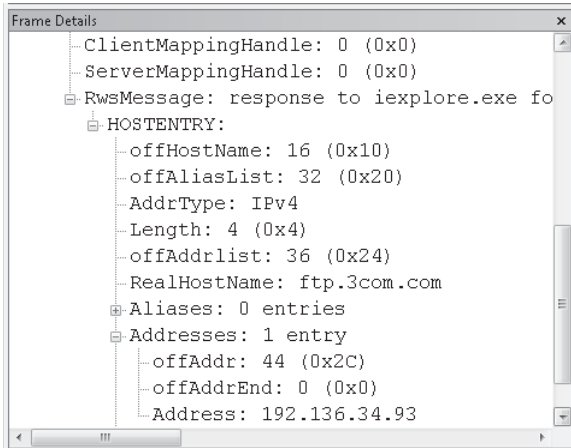


FIGURE 33-15 IP address in the Host Entry response message

Using Network Monitor, you've helped your colleague answer both of his questions—how IE is able to resolve the FTP server name to an IP address and why IE fails to display a directory listing of the FTP server. Although you are unable to explain why IE chooses not to connect to the FTP data channel listener described by the FTP server, you have demonstrated that IE fails to behave as expected based on the conversation with the FTP server. When your colleague contacts Microsoft Customer Support Services (CSS) to inquire about IE misbehavior, he can describe this problem clearly and in great detail. This information goes a long way in helping the CSS engineer determine the proper resources to engage on behalf of the caller.

Summary

In this chapter you learned how important it is to use Network Monitor in order to capture network traffic to troubleshoot TMG related problems. You learned how to configure Network Monitor via GUI and also via command-line interface. To demonstrate the full potential of Network Monitor, two scenarios were covered and there you were able to explore Network Monitor features such as filter syntax, view frame summary, and details. Throughout this exercise you also learned how to perform a step-by-step data analysis using Network Monitor and the correct approach to analyzing captures of different protocols.

Index

Symbols and Numbers

.iis, logging, 807–08
.NET Framework, 108, 171
.Save(), 835
.vhd files, 25
.w3c, logging, 807–08
32-bit platforms, 5, 36–37, 94
3-Leg Perimeter, 30, 67–68, 223
401-Unauthorized, 875
5-tuple, 72, 209–10
64-bit platforms, 5, 11–12, 36–37, 94

A

A records, DNS, 290–91
AAM (Alternate Access Mapping), 664–65, 689
Accept, HTTP, 915–16
Access control. *See also* Authentication; Filtering;
Internet; Remote access
alternate access mapping, 664–65
CERN proxy HTTP, 242–49
Configure Client Access, 188
NAT relationships, 216
ping requests, 212–15, 242–45
Policy Reevaluation, 249–53
proxy servers, 921
quarantined VPN clients, 31, 91, 223, 753
server publishing and, 577
SharePoint Services, 663
TMG, new features, 17
traffic policy behavior, 80–81, 241–49, 253–62
troubleshooting access rules, 253–62
UAG, security and, 26
URL filtering, overview, 465–70
user groups, 663
Web Access Policy, 185, 188–90, 194, 562–64, 568
Access Rules, network designs for, 80–81, 109
Accumulator, 13
Active caching, 920
Active Directory, 61, 93, 663–64, 741
Active Directory Lightweight Directory Services
(AD LDS), 147, 165, 171, 186–87
Active Directory Lightweight Directory Services
Server Role, 37
Active-active mode, 79
Active-passive mode, 78–79
ActiveX, 489–90
AD LDS (Active Directory Lightweight Directory
Services), 147, 171, 186–87
AddHttpsFrontEndOn, 702
Add-ins, TMG console, 186
Additional Security Policy, 188
Address Range Rule Element, 313
Address Resolution Protocol (ARP), 211–12
Addresses
DIP (Dedicated IP address), 285, 290
excluded, Single NIC firewalls, 70
gethostbyaddress, 121
installation, TMG 2010, 162–64
installation, TMG MBE, 149–51
intra-array addresses, configuring, 415–16
IP Allow List, 502–03
IP Allow List Providers, 503–05
IP Block List, 505–06
IP Block List Providers, 506
IP routing, basic, 210–15
logging, 806
Malware Inspection configuration, 435
managing and aggregating, 918–19
name resolution, 37–39
NAT relationships, 215–20
non-Web servers, 640
preinstallation checklist, 141
SharePoint Services, 662

- TMG networks, configuring, 56
- VIP (Virtual IP addresses), 285, 290, 498, 606
- VPN connections, 735
- Web proxy clients, 108
- Alerts
 - definition updates, 485
 - flood mitigation, 334, 338–40
 - Intrusion Detection System (IDS), 324–26
 - NLB (Network Load Balancing), 303
 - Policy Enforcement, 252
 - SharePoint Services, 664–65
 - spoofed packets, 54
 - SYN attacks, 338–40
 - TCP connections, worm attacks, 323
 - troubleshooting tab, 859
- All port scan attack alert, 326
- Allow policies, new features, 16
- Alternate Access Mapping (AAM), 664–65, 689
- AnnaKournikova virus, 488–90
- Anonymous public proxy servers, 534–38
- Anonymous requests, HTTP, 877
- Anti-malware. *See* Malware; Malware protection
- Anti-spam. *See* Spam
- Antivirus. *See* Virus protection
- Application filters. *See also* Filtering
 - application signatures, 561–70
 - protocol mapping, 50
 - publishing and, 573
 - SecureNET clients, 115, 118
 - server publishing, 576–77, 590
 - Session Initiation Protocol (SIP), 18
 - Single NIC firewalls, 70
 - TMG console, 191
- Application-layer firewalls, 10. *See also* Network Inspection System (NIS)
- Application-layer inspection, 308
- Applications. *See also* Application filters
 - access, TMG, 27
 - firewall rules, 24
 - mapping, 49
 - protocols, traffic profile, 47–51
 - Session Initiation Protocol (SIP) filtering, 18
 - TMG deployment options, 52–53
 - UAG, security and, 26
 - Winsock API calls, 121–22
- Architecture
 - COM (Component Object Model), 829–34
 - IAG 2007, 23–24

- NLB (Network Load Balancing), 285–88
 - TMG Setup, 169–72
- ARP (Address Resolution Protocol), 210–12
- Array Object, 830–31
- Arrays
 - CARP (Cache Array Routing Protocol), 80, 358–60, 362–64, 395–97, 413–17
 - DNS configuration, 289–91
 - DNS round-robin, 73, 75, 82, 349
 - Join Array and Disjoin Array Wizards, 203–04
 - log files, 812–13
 - migration, 88
 - policies, 299
 - synchronization, 297
- Assymetric bridging, 584
- Attachment files, 519–22
- Attacks. *See also* Malware Inspection; Virus protection
 - buffer overflow, 489
 - DNS attack detection, 326
 - flood mitigation, 330–36
 - preconfigured attack protection, 337–40
 - teardrop attacks, 329
- Audio streams, new features, 18
- Auditing, 373
- Authentication. *See also* Certificates; Signatures; Virtual Private Networks (VPN)
 - anonymous requests, 877
 - cache rules, 406
 - client selection and, 133
 - downgrade attack, 258
 - Exchange Server, 699–702, 705–06
 - failures, 652–53
 - HTTP
 - delegation, 883
 - dual, proxy and server, 881
 - overview, 874–83
 - proxy authentication, 879–80
 - server authentication, 878–79
- HTTP Filter
 - configuring, overview, 550–52
 - extensions, 555–56
 - headers, 557–60
 - inbound access, validating, 560–61
 - methods, 553–55
 - signatures, 561–70
- HTTPS Inspection
 - common errors, 548–49
 - configuring, 534–47

- IAS (Internet Authentication Services), 171
- L2TP over IPsec, configuring, 775
- logging, configuring, 806
- migration, 94
- NTLM and Exchange Server, 707
- Policy Enforcement, 253
- preinstallation checklist, 141
- protected networks, 233–39
- Require All Users To Authenticate, 238–39
- requirements, 39–40
- SecureNET clients, 118
- SharePoint Services, 663–64
- smart-cards, 719–20
- Test Rule, publishing, 612
- TMG Client, 132
- troubleshooting access rules, 256–62
- UAG, security and, 26
- VPN connections, 735–36, 741, 750–51
- Web listener, 580, 602–03
- Web Proxy Application Filter, 529–32
- Web publishing, 584–86
- web-proxy requests, 103
- Authentication Delegation, 585–86, 609, 635, 653, 669, 676, 686
- Authentication Header protocol, 735
- Authority, new features, 16
- Authorization, 26, 874–83. *See also* Access control
- Automatic Configuration Script, 376, 379
- Automatic discovery, 81–82, 93. *See also* WPAD (Web Proxy Automatic Discovery)
- Automatic Proxy Cache, 379–80
- Automatic updates, 315. *See also* Updates
- Automation, scripting, 836–42, 845–48.
 - See also* Scripting
- Auto-negotiation, 145
- AutoProxy. *See* WPAD (Web Proxy Automatic Discovery)
- autorun.hta, 171
- autorun.inf, 171
- Availability. *See also* Performance; Redundancy
 - load balancing
 - configuring, 293–98
 - enabling, 288–92
 - ISP redundancy, 263–65, 267–84
 - link availability testing, 265–67
 - NLB architecture, 285–88
 - post-installation best practices, 298–99
 - troubleshooting, 301–06
 - virtual environments, 300–01

- network design
 - for Access Rules, 80–81
 - for publishing rules, 76–80
 - overview, 71–76
- UAG, 26
- VPN access, 738–39

B

- Back firewalls, 31, 52, 68–69, 223, 335
- Back-to-back firewalls, 335
- Backup, network mapping, 48
- Backward compatibility, 37
- Basic authentication, 878. *See also* Authentication
- Basic trunks, 24
- BDA (Bidirectional affinity), 74, 288
- Behavioral Intrusion Detection, 196–97, 327
- Behavioral monitoring. *See also* Alerts; Logging; Performance
 - overview, 43–44
- Berkeley Sockets. *See* Winsock
- Best Practices Analyzer (BPA), 858–61
- Bidirectional affinity (BDA), 74, 288
- Bidirectional UDP protocols, 574
- bind (), 121
- Bing Safe Search, 471, 476
- Bits per connection, 704
- Block Expired Certificate, 545
- BootP clients, 18
- BPA (Best Practices Analyzer), 858–61
- BPA2Visio, 861
- Bridging, 583–84
- Broadcast domain, 287
- Broadcast protection, 338
- Broadcast, name resolution, 58–59
- Browsers
 - Automatic Proxy Cache, 379
 - client-side CARP, 396–97
 - embedded scripts, 489
 - parameters, 233
 - preinstallation checklist, 145
 - Web proxy clients, overview, 107–13
 - Winsock usage, 130–31
 - worm attacks, 489
 - WPAD (Web Proxy Auto Discovery) configuration, 364–79, 381

BubbleBoy virus, 489–90. *See also* Virus protection
Buffer overflow attacks, 489
Built-in networks, 222–24

C

Cache Array Routing Protocol (CARP)

- action examples, 949–54
- CARP logic, 947–49
- CARP Name System, 360
- cfile script, 362–64
- configuring, 413–17
- load factor, 359–60, 416–17
- MakeCARPExceptions, 358
- overview, 395–97

Caching

- Automatic Proxy Cache, 379–80
- Cache-Control field, 420, 916–17
- cache-control headers, 248–49
- CacheDir, 420–21
- compressed content, 393–94
- configuring
 - add cache rule, 400–07
 - add content download job, 407–12
 - CARP, 413–17
 - Enable Web Caching, 397–400
- DNS (Domain Name Service), 63
- FetchURL, 421
- IIS requests, 24
- internal name, 39
- monitoring, 394–95
- performance counters, 937, 939
- proxy servers, overview, 387–89, 919–20
- rebuilding, 421–22
- reverse caching, 391, 394–95, 920
- rules for, 391–92
- scenarios, 390–91
- settings, 398–400, 407–12
- SharePoint Services, 663
- storage, 389
- temporary disk cache, 429
- TMG console, 185, 190
- troubleshooting, 417–23
- web objects, 392
- Web Proxy Application Filter, 529

Caching Compressed Content Filter, 394

Capacity Planner, 592–93

CAP (Windows Crypto API), 535

CARP (Cache Array Routing Protocol)

- action examples, 949–54
- CARP Logic, 947–49
- CARPNameSystem, 360
- cfile script, 362–64
- configuring, 413–17
- load factor, 359–60, 416–17
- MakeCARPExceptions, 358
- overview, 395–97

CarpNameSystem, 360

CERN proxy requests, 107–13, 242–49, 384, 649–50, 877, 923. *See also* WPAD (Web Proxy Automatic Discovery)

Certificate Authorities, 535

Certificate Import Wizard, 621–25

Certificate Verify Message, 888

Certificates. *See also* Authentication; Signatures

- authentication, protected networks, 237
- Block Expired Certificate, 545
- cloned, 535
- Exchange Server, 699–700
- file formats, 619
- HTTP Filter
 - configuring, overview, 550–52
 - extensions, 555–56
 - headers, 557–60
 - inbound access, validating, 560–61
 - methods, 553–55
 - signatures, 561–70
- HTTPS Inspection
 - common errors, 548–49
 - configuring, 534–47
- installing, 619–25
- L2TP over IPsec, configuring, 775
- Listener SSL Certificates, 628
- migration, 91
- proxy migration, 93
- publishing rules, 595
- revocation, 793
- SSTP, 766
- Test Rule, publishing, 612
- TMG, new features, 16
- Web listener errors, 653–56
- Web Proxy Application Filter, 529–32
- Web servers, HTTPS protocol, 618

cfile, 345, 352–64

Chaining, 191, 922

- Change tracking, 798, 859
- CHAP (Challenge Handshake Authentication Protocol), 736
- Checksum offloading settings, 268
- Cipher Spec, 888
- Cipher Suite, 885–86
- Circuit-level firewalls, 10
- Class ID (CLSID), 488
- Client Access Server, 698
- Client certificate, 887–88
- Client Certificate Authentication, 663–64
- Client hello, 885
- Client Key Exchange Message, 888
- Clients. *See also* Remote access
 - access, 698–99, 747–56
 - acknowledgement, 888
 - applications
 - Automatic Proxy Cache, 379–80
 - AutoProxy in managed code, 384–85
 - Internet Explorer, 375–79
 - TMG Client, 381–82
 - Windows Media Player, 353, 382–84
 - choosing, 132–34
 - client CARP, 363, 396–97
 - Configure Client Access, 188
 - Exchange Server, 698–99, 704
 - Forefront TMG Client (TMGC), 119–32
 - HTTP Filter, 533–34
 - NLB (Network Load Balancing), 291–92
 - requests, single NIC firewalls, 70
 - SecureNET client, 113–18
 - TMG Client authentication, 132
 - VPN access, 738
 - Web proxy clients, 107–13, 132
- CLSID (Class ID), 488
- CNAME, 292–93, 376
- CNG (Cryptography Next Generation), 619
- Collision domain, 287
- COM (Component Object Model), 47–51, 266, 322, 829–34, 842–48
- Common Name (CN), 662
- Common Vulnerabilities and Exposures (CVE), 310
- Compatibility, backward, 37
- Component Object Model. *See* COM (Component Object Model)
- Compression, 393–94, 529–31, 885, 937, 953
- Compression Filter, 393–94
- Conditional forwarder, 60–61
- Conficker, 316–17, 567–70. *See also* Malware protection
- Confidentiality, UAG, 26
- Configuration file (cfile), 345, 352–64
- Configuration Storage Server (CSS), 289
- Configuration Storage Service (CSS), 165
- Configuration URL, 81–82
- Configure E-mail Policy Wizard, 205
- Configure SIP Wizard, 205
- Configure Web Access Policy Wizard, 397–400
- Configuring
 - caching
 - add cache rule, 400–07
 - add content download job, 407–12
 - CARP, 413–17
 - enable web caching, 397–400
 - Configure Global Link Translation, 190
 - Configure Radius Server Settings, 190
 - Deployment Wizard, 202–03
 - DNS attack detection, 326
 - Enhanced NAT (E-NAT), 820–26
 - Exchange Server, 707–18
 - Firewall Chaining options, 191
 - Firewall Client Settings, 191
 - flood mitigation, NIS, 330–36
 - HTTPS Inspection, 534–47
 - IDS (Intrusion Detection System), 324–26
 - IP preferences, NIS, 327–30
 - LDAP Server Settings, 190
 - load-balancing, ISP Redundancy, 276–84
 - Malware Inspection, one-time reports, 446–50
 - Malware Inspection, recurring reports, 451–55
 - networks
 - creating networks, 222–31
 - network relationships, overview, 209–22
 - protected networks, 231–39
 - NIS (Network Inspection System), 311–16, 327–36
 - NLB (Network Load Balancing), 276, 293–98
 - SharePoint Services
 - multi-server, 672–79
 - overview, 665–66
 - server farm, 679–89
 - single-server, 667–72
 - SMTP protection, overview, 493–94
 - spam filtering, 502–18
 - TMG console, 185–87
 - TMG logging, 800–09
 - TMG networks, 54–57

Conflicts

- TMG Setup
 - architecture, 169–72
 - setup options, 172–74
- Update Center, 481–85
- URL filtering, 470–78
- virus and content filtering, 518–27
- VPN
 - dial-in clients, 747–63
 - site-to-site, 774–81
 - SSTP, 763–71
- WLBS display, 305
- WPAD (Web Proxy Auto Discovery), 364–79
- Conflicts
 - IAG, ISA Server, 24
 - LSP (Layered Service Providers), 125
 - write conflicts, cache and, 389
- CONNECT, 871, 913
- Connect to Forefront Protection Manager 2010 Wizard, 204–05
- Connection Properties, 281
- Connection table, exploitation of, 323
- Connection, HTTP, 916
- Connectivity. *See also* Access control;
Intrusion detection
 - access, enabling, 22–23
 - ISP Redundancy, 264
 - logging, 813–14
 - SecureNET clients, 115–17
 - Web Publishing, availability, 77
- ConnectivityRemoteVerificationPort, 267
- Content Filtering, 507–11, 515, 518–27
- Content for Offline Browsing, cache, 405
- Content Requiring User Authentication
 - For Retrieval, 406
- Content, HTTP, 914–15
- Content-encoding, 915
- ConvertUrlToLowerCase, 355–56
- cookieauthfilter.dll, 702–03
- Cookies, 73, 77–78, 587
- Coordination, migration and, 94
- Counters
 - cache, 395, 939
 - compression performance, 953
 - DiffServ, 954
 - e-mail hygiene, 960
 - Firewall packet engine, 938
 - H.323 filter, 939
 - how to use, 964
 - HTTPS performance, 959
 - malware protection, 956
 - Microsoft Firewall service, 941
 - overview, 937–38
 - requirements, 41
 - SOCKS filter, 943
 - TMG Performance Monitor, 962
 - URL filtering, 961
 - Web proxy, 944
- CPU load, flood mitigation, 330–36
- Create VPN Site-To-Site Connection Wizard, 775–80, 782–87
- Creating
 - HTTPS Web listeners, 625–30
 - Malware Inspection reports, 446–63
 - network rules, 226–31
 - networks, 222–31
 - Non-Web Server Publishing rule, 637–47
 - reports, new features, 15
 - Web publishing rule, secure, 630–36
 - Web site publishing rules, 558
- Credentials. *See also* Authentication; Certificates;
Signatures
 - Exchange Server, 700–02
 - HTTP, overview, 874–83
 - integrated authentication, 235–36
 - requirements, 39–40
 - TMG Client, 132
 - Web publishing, 585–86
- Cryptography Next generation (CNG), 619
- CSS (Configuration Storage Server), 289
- CSS (Configuration Storage Service), 165
- Customer Feedback, 203
- CVE (Common Vulnerabilities and Exposures), 310

D

- Data transfer, Winsock, 119
- DBCS (double-byte character set), 552
- DCOM (Distributed Component Object Model), 47–51
- Dedicated IP address (DIP), 285, 290
- Dedicated Servers List, ISP, 278, 282
- Default gateway, 268
- Default internal networks, 54–57
- Default IP Address, 219

- Deflate algorithms, 393–94
- DELETE, 871, 913
- Delete wpad command, 93
- Demilitarized zone (DMZ), 67–68
- Denial of Service (DoS) attack, 323, 333–34
- Deny policies, new features, 16
- Deployment
 - client selection and, 132–33
 - network relationships, overview, 209–22
 - TMG, 27–28
 - TMG option, networks, 51–53
 - UAG (Forefront Unified Access Gateway), 25, 27–28
 - virtual environments, 44–45
- Deployment Wizard, 200, 202–03
- DHCP (Dynamic Host Configuration Protocol), 93, 268, 346–50, 366–69
- DHCP NFORM request, 369
- DhcpRequestParams (), 346–47
- Diagnostic Logging Events, 859. *See also* Logging
- Dial-in users, RADIUS, 40, 237–38, 663–64, 751
- Dial-in VPN clients, 31, 52–53, 91–92, 663–64, 741, 762–63
- DiffServ performance counter, 937, 954
- Digest authentication, 234, 878
- DIP (Dedicated IP address), 285, 290
- Dir1.cdat, 389
- Disjoin Array Wizard, 203–04
- Disk Write Queue Length, 42
- Disks
 - caches, 389
 - flood mitigation, 330–36
 - forward caching, 390
 - hardware requirements, 35–36
 - log files, 803–04, 812–13
 - mirroring, 813
 - performance, 41–42
 - reverse caching, 391
 - striping, 813
 - temporary disk cache, 429
- Distributed Component Object Model (DCOM), 47–51
- DLL (dynamic-linked library), 122–25
- DMZ (demilitarized zone), 67–68
- DNS (Domain Name System)
 - attack detection, 326
 - cache, 63
 - configuring WPAD, 369
 - DNS round-robin, 73, 75, 82, 95, 349
 - ISP Redundancy, 78–79
 - migration, 92–93, 95
 - name resolution, 38, 58–63
 - NLB (Network Load Balancing), 289–91
 - publishing, 574
 - reverse lookup, 516
 - Root Servers, 265–67
 - SecureNET clients, 115–17
 - server publishing, 590
 - site-to-site (S2S) VPN migration, 92
 - STMP lookup, 820
 - WPAD (Web Proxy Auto Discovery), 93, 350–52
- DNS Alias, 376
- DNS Server, 332
- DNS Server Global Query Block List, 374
- DNS Server Publishing, 326
- DNS System Log, 372
- dnscmd command, 371
- Domain controllers, 39–40, 701
- Domain isolation, 53
- Domain membership, migration and, 94
- Domain Name System. *See* DNS (Domain Name System)
- Domains, joining to firewalls, 82–84
- Double-byte character set (DBCS), 552
- Download Job Wizard, 409–12
- Downloads
 - .vhd files, UAG deployment, 25
 - audio and video streams, 18
 - cache, content download jobs, 407–12
 - TMG, new features, 14, 18
 - Trivial File Transfer Protocol (TFTP) filter, 18
 - Web proxy client requests, 113
- Drivers, preinstallation checklist, 141
- Duplex, 78
- Dynamic Content, 405
- Dynamic Host Configuration Protocol (DHCP), 93, 268, 346–50, 366–69
- Dynamic links, alternate access mapping, 664–65
- Dynamic load balancing, new features, 19. *See also* Network Load Balancing (NLB)
- Dynamic update, 370–74
- Dynamic-linked library (DLL), 122–25

E

- EAP (Extensible Authentication Protocol), 736
- EAS (Exchange Active Sync), 698–99, 704, 706–07, 718, 721

Echo requests

- Echo requests, 212–15, 242–45
- ECN (Explicit Congestion Notification), 144
- Edge firewalls
 - deployment options, 52
 - designing, 29–30
 - Network Inspection System (NIS), 335
 - network rules, 220–22
 - network template, 223
 - template, 66–67
 - tunneling protocols, 22–23
- Edge Malware Protection (EMP), 13, 429, 469, 799
- Edge Malware Protection (EMP) Scanner, 13
- Edge Transport Server, 698
- Egress migrations, 90–95
- E-mail. *See also* E-NAT (Enhanced NAT)
 - alerts, SharePoint Services, 664–65
 - E-mail Policy, 192, 194–95, 205
- Exchange Server
 - configuring, 707–18
 - publishing, planning for, 697–707
 - troubleshooting, 719–30
- hygiene performance counter, 938, 960
- protection
 - configuring virus and content filtering, 518–27
 - SMTP protection, 490–501
 - spam filtering, configuring, 502–18
 - threat overview, 487–90
- servers, 16–17, 47–51
- E-Mail Policy Wizard, 205, 495–501
- E-Mail Protection Wizard, 494–501
- Embedded scripts, 489–90
- EMP (Edge Malware Protection), 13, 429, 469, 799
- Enable ISP Redundancy Wizard, 206
- E-NAT (Enhanced NAT)
 - configuring, 820–26
 - ISP Redundancy, 265, 268
 - overview, 817–20
 - troubleshooting, 826–27
- Encryption. *See also* Tunnels, VPNs
 - Cipher Spec, 888
 - control channel communication, 127
 - Exchange Server, 699–700, 703
 - SecureNET clients, 115
 - SharePoint Services, 662–63
 - tunneling protocols, 22–23
- Enhanced NAT. *See* E-NAT (Enhanced NAT)
- Enterprise policies, locating arrays, 837
- Enumerated port scan attack alert, 326

- Errors
 - 691, 743
 - 766, 793
 - 789, 793
 - 806, 793
 - 809, 793
 - reading logs, 177
 - scripting practices, 835
 - TMG Setup failure, 181–84
- Ethernet, IP routing, basic, 210–15
- European Institute for Computer Antivirus Research (EICAR), 443
- Events
 - 5783 event, 897
 - DNS System Log, 372
 - flood mitigation, 339–40
 - Windows Event Logs, 862
 - WLBS display, 305
- EWS (Exchange Web Services), 723
- Exchange (Anti Spam), 479
- Exchange Active Sync (EAS), 698–99, 704, 706–07, 718, 721
- Exchange Hub Transport Server, 523
- Exchange Intelligent Message Filter, 490–91
- Exchange Outlook Anywhere Services, 77
- Exchange Outlook Web Access, 76–78
- Exchange Publishing Wizard, 698–700
- Exchange Server
 - configuring, 707–18
 - publishing, planning for, 697–707
 - SPAM protection, 491
 - troubleshooting, 174, 719–30
- Exchange Web Services (EWS), 723
- ExchangeVersion, 702–03
- Exchange Publishing Wizard, 702–03
- Explicit Congestion Notification (ECN), 12, 144
- Explicit content, 471
- ExpMatch(), 949
- Exporting files, 838
- Extensible Authentication Protocol (EAP), 736
- External Mail Routing Configuration, 498
- External networks, 80, 223–24. *See also* Networks

F

- Failback, ISP Redundancy, 267
- Failed DNS Resolutions counter, 58

- Failover. *See also* Availability; Load balancing
 - ISP failover, 82, 263–65
 - ISP Redundancy, 78–79, 267, 269–76
- FailuresToUnavailable, 267
- Fast trickling, 438–39
- Fault tolerance, new features, 19
- FCS (Forefront Client Security), 799
- FetchURL, 421
- File and Printer Sharing, 144
- File Transfer Protocol (FTP), 18, 113. *See also* TFTP
 - (Trivial File Transfer Protocol) Filter
- File-based antivirus, 440. *See also* Virus protection
- Files
 - attachments, 519–22
 - extensions, 487–90, 519–22, 533–34, 555–56
 - filtering, 519–22
 - importing and exporting, 838
 - logging, 803–04
 - Session Initiation Protocol (SIP) filtering, 18
 - SharePoint Services
 - multi-server, configuring, 672–79
 - overview, configuring, 665–66
 - planning for publishing, 661–65
 - server farm, configuring, 679–89
 - single-server, configuring, 667–72
 - troubleshooting, 689–95
- Filtering. *See also* E-mail protection; HTTP Filter;
 - Malware Inspection
- applications, 18, 50, 70, 110, 115, 118, 191, 561–70, 573, 576–77, 590
- Caching Compressed Content Filter, 394
- Compression Filter, 393–94
- configuring virus and content filtering, 518–27
- Content Filtering, 507–11
- DNS attack detection, 326
- file filtering, 519–22
- Forms-Based Authentication filter, 702–03
- HTTP Malware filter, 12–13
- ISAPI, 23–24
- link translation, 583
- Message Body Filtering, 523–27
- Network Monitor captures, 899–903
- Network Monitor, SOCKS-proxy troubleshooting, 903–09
- packet filters, RRAS, 748
- performance counters, 937–39, 943
- Recipient Filtering, 512–13
- Sender Filtering, 513–15
- server publishing, 590
- Session Initiation Protocol (SIP), 18
- spam, configuring, 502–18
- TMG console, 191
- TMG SMTP filter, 491
- traffic, overview, 6–8
- Trivial File Transfer Protocol (TFTP), 18
- URLs
 - configuring, 470–78
 - new features, 15–16
 - overview, 465–70
 - Update Center, 478–81
 - Update Center, configuring, 481–85
 - Web access policy, 194
- Virus Filtering, 522–25
- Web filters and publishing, 578–80
- Web Proxy Application Filter, 529–31
- Web proxy filter, 265
- FindProxyForUrl, 362–64, 379
- FindProxyForURLEx, 362–64
- Firewall generation, defined, 10
- Firewalls
 - chaining, 335
 - client considerations, NLB, 293
 - Firewall Client, 93, 253, 335, 384
 - Firewall Policy, 188, 194
 - log fields, 798–800
 - packet engine performance counters, 937–38
 - policy rules, basics, 242
 - types of, 9–10
 - URL filtering, 469
- Flood attacks, 323, 329–36
- Forefront Client Security (FCS), 799
- Forefront Protection 2010 for Exchange Server, 491
- Forefront Protection Manager 2010 (FPM), 15
- Forefront Security for Exchange (FSE), 479
- Forefront Threat Management Gateway. *See* Microsoft
 - Forefront Threat Management Gateway (TMG)
- Forms-Based Authentication, 580, 663–64, 700–03
- Forward caching, 390, 394–95, 920. *See also* Caching
- Forward proxy, 921
- Forwarders, 60–61
- FPC.Root, 830
- FPCArray, 830
- FPM (Forefront Protection Manager 2010), 15
- FQDN (Fully Qualified Domain Name), 299, 806
- Front Firewall, network templates, 223
- FTP (File Transfer Protocol)

- commands, 905–06
- filters, 50
- servers, 583–84, 590
- TMG deployment options, 52–53
- Web proxy clients, 113

Full-duplex, 78

Fully Qualified Domain Name (FQDN), 299, 806

G

Gates, Bill, 490

Generic Application Protocol Analysis (GAPA), 17, 307

Generic Network Intrusion System (NIS),
 new features, 17

Generic Routing Encapsulation (GRE), 117, 734

GET, 871, 913

getaddrinfo, 121, 125

gethostbyaddress, 121, 125

gethostbyname, 121

GetHostByName(), 350

Getting Started Wizard, 54–57, 66–67, 69–70, 174,
 200–01

Global HTTP Policy Settings, 190

Global Link Translation, 188, 190

Global Query Block List, 371

Global URL filtering, configuring, 472–75

GRE (Generic Routing Encapsulation), 117, 734

Group policies

- automatic discovery, Internet Explorer, 377–79
- availability, network designs, 81
- SharePoint Services, 663
- traffic, 7

GZIP, 393–94

H

H.323 filter performance counter, 939

H.323 filters, 590

Half open attack, 333

Half-duplex, 78

Handshakes, 870, 884

Hardware

- load balancing, migration and, 95
- preinstallation checklist, 141
- requirements, 35–36
- VPN access requirements, 739–41

HEAD, 871

Headers

- Authentication Header Protocol, 735
- cache-control headers, 248–49
- HTTP, 873
- HTTP Filter, 533–34, 557–60
- malformed, 489
- Maximum Headers Length, 551
- web objects, caching, 392

HELO/EHLO analysis, 516

High Bit Characters, 552

HNode (hybrid node type), 59

Host mismatch, 650–51

HTML e-mail, 489–90

HTML forms-based authentication, 701

HTML progress page, 14

HTTP (Hypertext Transfer Protocol). *See also* HTTP
 Filter; HTTPS

- anonymous requests, 877
- authentication, 663–64, 874–83
- CERN proxy traffic, 242–49
- compression, caching, 393–94
- dual authentication (proxy and server), 881
- Global HTTP Policy Settings, 190
- header, cache information, 418
- libraries, 353
- NTLM authentication, 881–82
- objects, caching, 392
- overview, 869–74, 911–17
- Policy Reevaluation, 249–53
- proxy authentication, 879–80
- requests, Web proxy clients, 109–11
- resources, client requests for, 110
- server authentication, 878–79
- SharePoint Services, 662–63
- traffic, 22–23, 31, 49, 52–53, 73
- Web listener, 580
- Web Proxy Application Filter, 529–32
- Web proxy clients, 113
- Web publishing, 581, 648
- Web server publishing, 600–18

HTTP 502 Bad Gateway, 549

HTTP Filter, 533–34

- CERN proxy example, 247
- configuring, 550–52
- extensions, 555–56
- headers, 557–60
- methods, 553–55

- signatures, 561–70
- validating inbound access, 560–61
- HTTP Malware filter, 12–13
- HTTP.SYS, 763
- HTTPS
 - Exchange Server, 699–700
 - exclusion list, 469
 - HTTPS Inspection
 - common errors, 548–49
 - configuring, 534–47
 - new features, 16
 - outbound traffic, 22–23
 - overview, 884–89
 - performance counters, 938, 959
 - SharePoint Services, 662–63
 - TMG deployment options, 52–53
 - Web listener, 580
 - Web Proxy Application Filter, 529–32
 - Web proxy clients, 113
- Hub Transport Server, 698
- Hybrid node type (HNode), 59

I

- IAG 2007, 23–24
- IANA (Internet Assigned Numbers Authority), 9
- IAS (Internet Authentication Services), 171
- ICF (Windows Internet Connection Firewall), 7
- ICMP Echo Request, 212–15, 242–45
- ICS (Internet Connection Sharing), 7
- IDP (ISA Data Packager), 861
- IDS (Intrusion Detection System)
 - configuring, 324–26
 - overview, 323
 - requirements, 40–41
 - TMG, new features, 17
- IGMP support, 287
- IIS (Internet Information Services), 23–24, 690
- IKE (Internet Key Exchange), 735–36
- ILOVEYOU virus, 488–90. *See also* Virus protection
- ImplementFindProxyForURL, 362–64
- Importing files, 838
- Inbound traffic, 22–23, 28–32, 264, 560–61.
 - See also* Traffic
- Incoming context, publishing, 573–74
- Inetinfo.exe, 24
- Ingress migrations, 90–95

- Installing
 - certificates, 619–25
 - TMG manual installation, 156–68
 - TMG MBE, manual installation, 145–56
 - TMG, preinstallation checklist, 141–45
 - TMG, setup architecture, 169–72
 - TMG, unattended installation, 168
- Integrated authentication, 235–36
- Integrated NLB (Network Load Balancing), 288–92
- Integration, overview, 8–9
- Integrity, UAG, 26
- Intelligent Application Gateway (IAG) 2007, 21
- Intermediate Certification Authority, 16
- Internal Certification Authority, 700
- Internal networks, 54–57, 222–24. *See also* Networks
- Internet. *See also* Internet Explorer
 - HTTP
 - anonymous requests, 877
 - authentication, 878, 883
 - dual authentication (proxy and server), 881
 - NTLM authentication, 881–82
 - overview, 869–74
 - proxy authentication, 879–80
 - server authentication, 878–79
 - HTTPS, overview, 884–89
 - Malware Inspection, testing, 443–45
 - preinstallation checklist, 145
 - timelines and milestones, 911
 - TMG deployment options, 52–53
 - traffic management, 48
 - Windows Libraries, 967
- Internet Assigned Numbers Authority (IANA), 9
- Internet Authentication Services (IAS), 171
- Internet Connection Firewall (ICF), 7
- Internet Connection Sharing (ICS), 7
- Internet Explorer. *See also* Internet
 - Automatic Proxy Cache, 379
 - client-side CARP, 396–97
 - embedded scripts, 489–90
 - parameters, 233
 - preinstallation checklist, 145
 - Web proxy clients, overview, 107–13
 - Winsock, 130–31
 - worm attacks, 489
 - WPAD (Web Proxy Auto Discovery), 364–79, 381
- Internet Information Services (IIS), 23–24, 690
- Internet Key Exchange (IKE), 735

- Internet Key Exchange version 2 (IKEv2), 736
- Internet Protocol Control Protocol (IPCP), 735
- Internet Protocol security (IPsec), 22–23, 52–53, 330, 735, 773–74, 790–92
- Internet Security and Acceleration (ISA) Server 2000, 490–91, 926–29
- Internet Security and Acceleration (ISA) Server 2004, 93, 363, 490–91, 929–31
- Internet Security and Acceleration (ISA) Server 2006, 93, 99–105, 490–91, 932–33
- Internet Server Application Programming Interface (ISAPI), 23–24
- Intranet Web publishing, 77
- Intrusion detection. *See also* Intrusion Detection System (IDS); Intrusion Prevention System (IPS)
 - requirements, 40–41
 - TMG console, 192, 196–97
- Intrusion Detection System (IDS)
 - configuring, 324–26
 - configuring DNS attack detection, 326
 - overview, 323
 - requirements, 40–41
 - TMG, new features, 17
- Intrusion Prevention System (IPS), 17, 322
- Intrusion prevention, new features, 15. *See also* Malware protection
- IP addresses
 - 3-Leg Perimeter networks, 68
 - 5-tuple, 209–10
 - basic routing, 210–15
 - configuring intra-array addresses, 415–16
 - dial-in VPN migration, 91
 - DIP (Dedicated IP address), 285
 - E-Mail Policy Wizard, 495–501
 - IP Allow List, 502–03
 - IP Allow List Providers, 503–05
 - IP Block List, 505–06
 - IP Block List Providers, 506
 - load balancing, 587–88
 - logging, 806
 - lookup performance, 38
 - Malware Inspection configuration, 435
 - managing and aggregating, 918–19
 - NAT relationships, 215–20
 - NIS (Network Inspection System), 327–30
 - non-Web servers, 640
 - server-side CARP, 397
 - SharePoint Services, 662
 - site-to-site (S2S) VPN migration, 92
 - SSTP, 766
 - TMGC configuration data, 127
 - VIP (Virtual IP addresses), 285
 - Web listener, 580, 602
- IP Allow List, 502–03
- IP Allow List Providers, 503–05
- IP Block List, 505–06
- IP Block List Providers, 506
- IP fragments, 329
- IP half scan, alert, 325
- IP protocols
 - 50 (ESP), 735
 - 51 (Authentication Header), 735
 - More Info, 9
 - TMGC as name service provider, 125
- IP subnet, 268
- ipconfig, 305
- IPCP (Internet Protocol Control Protocol), 735
- IPS (Intrusion Prevention System), 17, 322
- IPsec, 22–23, 52–53, 330, 735
- IPsec ESP, 790–91
- IPsec NAT-T, 735, 791–92
- IpSubnet, 362
- ISA 2004, 90
- ISA 2006, 90
- ISA Data Packager (IDP), 861, 892
- ISA Info Viewer, 702–03
- ISA server
 - migration, 88
- ISA Server
 - IAG 2007 integration, 24
 - overview, 10–11
 - traffic filtering, 6–8
- ISA Server 2000, 490–91, 926–29
- ISA Server 2004, 93, 363, 490–91, 929–31
- ISA Server 2006, 93, 99–105, 490–91, 932–33
- ISA Server 2006 Supportability Update, 3
- ISA Setup files, 156
- ISA_GettingStarted_XXX.log, 175
- ISA_IpsUpdateInstall.log, 175
- ISAADAM_IMPORTSCHEMA_XXX.log, 175
- ISAADAM_INSTALL_XXX.log, 175
- ISAFWSV_XXX.log, 175, 177, 181
- ISAFWUI_XXX.log, 175
- ISAPI (Internet Server Application Programming Interface)
 - filtering, 23–24

- ISAPI Extension
 - IAG 2007, 23–24
- ISASCHED Service, 481
- isatap queries, 371
- ISATools.org rule, 406
- IsaUpdateAgent.log, 175
- ISAWRAP_XXX.log, 175–76
- isIpv6, 362
- ISP 1 Dedicated Servers List, 278
- ISP 2 Dedicated Servers list, 282
- ISP connections
 - Enable ISP Redundancy Wizard, 206
 - failover, 82, 263–65, 267
 - load balancing, 264, 267
 - TMG, new features, 19
- ISP Link 1 Connection Properties, 278
- ISP Redundancy
 - Enable ISP Redundancy Wizard, 206
 - hardware requirements, 35–36
 - overview, 78–79, 263–65
 - rule basics, 242
 - TMG console, 197–98
 - UAG, security, 26
- ISP Redundancy Configuration Wizard, 269–74, 276–84
- ISPRedundancyConfig, 266

J

- Join Array Wizard, 203–04
- JScript
 - containers, 359
 - importing and exporting files, 838
 - locating arrays, 837
 - objects, 357–59, 361
 - overview, 834
 - WPAD, cfile, 352–64
- JScript Regular Expressions, 362

K

- KaK worm, 489–90
- Keep-Alive, 916
- Kerberos authentication, 39–40, 878
- Kerberos Constrained Delegation (KCD), 669–70, 701

- Kernel mode, IIS requests, 24
- Keyword list, 527

L

- L2TP (Layer 2 Tunneling Protocol), 22–23, 52–53, 330, 736–37
- L2TP/IPsec (Layer 2 Tunneling Protocol)
 - configuring, 774–81
 - overview, 735
 - site-to-site VPN connections, 773–74
 - troubleshooting, 790–93
- LAN (Local Area Network), 56, 143, 592–93.
 - See also* Networks
- Land, alert, 325
- Large logging queue (LLQ), 814
- Latin 1 characters, 552
- Layer 2 Tunneling Protocol (L2TP), 22–23, 52–53, 330, 736–37
- Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec), 735, 773–81, 790–93
- Layered Service Providers (LSPs), 122–25
- LDAP server, 40, 190
- Legacy settings, Internet Explorer and WPAD, 381
- Libraries, Windows Internet, 967
- Licenses
 - Malware Inspection, 441
 - Update Center, 481
- Lightweight Directory Services (LDS), 37, 147, 165, 171, 186–87
- Link translation, 583, 664–65
- listen, 121
- Listener SSL Certificates, 628
- Listeners
 - HTTPS Web listeners, 625–30
 - migration, 90–91
 - Network Listener, 589
 - server publishing, 574–76
 - Web listeners, 580, 600–01, 766
 - Web Proxy Application Filter, 529
 - Web publishing, 578–80
- LMHOSTS, 59
- Load balancing. *See also* Availability
 - CARP load factor, 416–17
 - DNS Round-Robin, 349
 - enabling, 288–92
 - flood mitigation, 336

- ISP Redundancy, 78–79, 263–65, 267–84
- link availability testing, 265–67
- migration and, 95
- new features, 19
- NLB architecture, 285–88
- NLB, configuring, 293–98
- post-installation best practices, 298–99
- publishing rules, 595–96
- troubleshooting, 301–06
- virtual environments, 300–01
- Web farms, 26, 587–88
- Web Publishing Load Balancing (WPLB), 72
- Web server publishing, 606
- Load Balancing Factor, 282
- Local Area Network (LAN), 56, 143, 592–93.
 - See also* Networks
- Local Host Access, 77
- Local Host networks, 222–24
- Local storage, 481. *See also* Storage
- Log Traffic Blocked By Flood Mitigation, 339–40
- Logging
 - best practices, 809–15
 - cache behavior, 417–20
 - configuring, 800–09
 - DNS System Log, 372
 - file and disk space controls, 803–04
 - firewall fields, new, 798–800
 - flood mitigation, 339–40
 - hardware requirements, 36
 - HTTP Filter, 566
 - importance of, 797–98
 - Intrusion Detection System (IDS), 324–26
 - local text, 807–08
 - Malware Inspection, 429–30, 446–63
 - queue, 809
 - reports, 446–63, 859
 - SharePoint Services, 692–95
 - storage, 41–42
 - TMG console, 192–93, 199
 - TMG Setup, 174–75
 - traffic simulator, 261–62
 - Web proxy fields, new, 798–800
- LogParser, 808
- Loopback, SecureNET clients, 116–17
- Loops, scripts, 835
- Loose Source Routing, 329
- LSPs (Layered Service Providers), 122–25

M

- MAC (Media Access Control), 210–15
- MAC-addresses, 8, 286
- Mail. *See* E-Mail; SMTP (Simple Mail Transfer Protocol)
- Mailbox Server, 698
- MakeCARPExceptions, 358
- MakeIPs, 357, 362
- MakeIps(), 362
- MakeNames, 358, 362
- MakeProxies(), 359
- Malware Inspection. *See also* Malware protection
 - configuring
 - content delivery, 438–39
 - environment considerations, 431–36
 - settings, 437–38
 - storage, 439–40
 - Internet access, testing, 443–45
 - license, 441
 - logging, 799
 - overview, 427–31
 - per-rule, defining, 442
 - reports, creating, 446–63
 - updates, 440, 478
- Malware protection. *See also* Malware Inspection
 - Conficker, 567–70
 - e-mail threats, overview, 487–90
 - MMPC (Microsoft Malware Protection Center), 308
 - MS08-067, 316–17
 - new features, 11–17, 27
 - performance counters, 938, 956
 - TMG console, 187
 - Update Center, 478–81
 - Web Access Policy, 188–90
- Management
 - applications, 49
 - disks, hardware requirements, 36
 - Forefront TMG Management Console, 5
 - new features, 14–16
 - NLB (Network Load Balancing), 288, 302–04
 - remote, setup options, 172–74
- Media Access Control (MAC), 210–15
- Media Player, 353, 382–84
- Melissa virus, 488–90. *See also* Virus protection
- Memory
 - caching, 389–91
 - flood mitigation, 330–36
 - log files, 803–04, 812–13

- requirements, 35–36
- TMG requirements, 12
- VPN access, requirements, 740–41
- Message Body Filtering, 523–27
- Message Queuing, 171
- Messaging. *See also* E-mail
 - Exchange Server
 - configuring, 707–18
 - publishing, planning for, 697–707
 - troubleshooting, 719–30
- Microsoft .NET Framework, 108, 384–85
- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), 736
- Microsoft Essential Business Server, 4
- Microsoft Exchange Edge Transport Role, 174
- Microsoft Exchange Server
 - configuring Exchange Client access, 707–18
 - publishing, planning for, 697–707
 - troubleshooting, 719–30
- Microsoft Firewall Service (wspv.exe), 469, 941
- Microsoft Forefront Threat Management Gateway (TMG)
 - Capacity Planner, 592–93
 - clients, features of, 135
 - Console, 5
 - deployment, overview, 5–6
 - feature comparison, 4
 - Firewall Packet Engine, 42
 - Firewall Service, 42
 - high availability, 79–80
 - installation, manual, 156–68
 - Management Console, 5
 - Medium Business Edition (MBE)
 - console, 185–91
 - deployment, 5
 - installation, manual, 145–56
 - migration, 90
 - new features, 11–14
 - new wizards, 199–206
 - overview, 933–35
 - MPEngine (Malware Protection Engine), 12–13
 - new features
 - e-mail, anti-malware, anti-spam support, 16–17
 - firewall integration, 8–9
 - firewall types, 9–10
 - HTTPS inspection, 16
 - network functionality, 18–19
 - network intrusion prevention, 17
 - Session Initiation Protocol (SIP) filter, 18
 - summary of, 19
 - TFTP filter, 18
 - URL filtering, 16
 - user interface, management and reporting, 14–16
 - Windows Server 2008 and 64-bit support, 11–14
 - overview, 3–4
 - Performance Monitor, 962
- Microsoft Forefront Unified Access Gateway (UAG), 25–26
- Microsoft Hyper-V, 25
- Microsoft Malware Protection Center (MMPC), 308, 316–17
- Microsoft Malware Protection Engine (TMG MPEngine), 12–13
- Microsoft Management Console (MMC), 51
- Microsoft Office 2003 Web Components, 37
- Microsoft Office Outlook, 353, 698–700, 705
- Microsoft Office Outlook Anywhere, 73
- Microsoft Office SharePoint Services
 - configuring
 - multi-server, 672–79
 - overview, 665–66
 - server farm, 679–89
 - single-server, 667–72
 - publishing, planning for, 661–65
 - troubleshooting, 689–95
- Microsoft Reputation Service (MRS). *See also* URL filtering
 - Bing safe search, 471
 - URL filtering, overview, 465–70
- Microsoft SmartScreen technology, 511
- Microsoft SQL Express, 37
- Microsoft SQL Server Native Client, 37
- Microsoft SQL Server Setup Support Files, 37
- Microsoft SQL Server Volume Shadow Copy Service (VSS) Writer, 37
- Microsoft Telemetry Service, 203
- Microsoft Update, 13, 465, 479–81, 484
- Microsoft Update Setup, 202
- Microsoft.Isa.ManagedPerfCounters.dll.log, 175
- Migration
 - checklists, 96–99
 - ISA 2006 SE to TMG 2010 EE Forward Proxy, 99–105
 - overview, 87–89
 - publishing scenarios, 90–91
 - scenarios for, 90–95
- MIME (Multipurpose Internet Mail Extension), 489

- MinimalResumeTime, 267
- Mirroring with striping, 813
- Mixed node types (MNode), 59
- MMC (Microsoft Management Console), 51
- MMPC (Microsoft Malware Protection Center), 308, 316–17
- MMS, 50, 382
- MNode (mixed node type), 59
- Mobile users, 27
- Monitoring, 186–87, 193, 319–21, 394–95.
 - See also* Logging
- More Info
 - A records, creating, 291
 - Active Directory and Group Policy administration, 7
 - ActiveSync in Exchange Server, 718
 - Alternate Access Mapping, 665, 689
 - application signatures, 561
 - ARP (Address Resolution Protocol), 210
 - attacks, 326
 - authentication methods, 806
 - authentication, downgrade attack, 258
 - authentication, Exchange Server, 702
 - authentication, mechanisms and delegations, 586
 - authentication, SharePoint Services, 664
 - authentication, web-proxy requests, 103
 - Automatic Proxy Result Cache, 380
 - auto-negotiation, 145
 - AutoProxy, 385
 - BadTrans, 490
 - bidirectional affinity, 288
 - Bing safe search, 471
 - cache counters, 395
 - cache file usage, 421
 - cache rules, 401
 - Cache-Control field, 420
 - certificate errors, troubleshooting, 656
 - certificate file format, 619
 - certificate requirements, 663
 - certificate revocation, 793
 - cfile extensions, Web proxy, 354
 - Cipher Suite, 886
 - client configuration, NAP, 763
 - CNAME as proxy server, 292
 - Conficker, 567
 - connectivity, SQL Server Database, 814
 - constrained delegation, configuring, 727
 - Content Filtering, 508, 516
 - Cryptography Next Generation (CNG), 619
 - CVE (Common Vulnerabilities and Exposures), 310
 - DHCP configuration, 368
 - DhcpRequestParams(), 347
 - digital certificates, 775
 - DNS lookup for STMP, 820
 - DNS Round-Robin, 349
 - DNS Server Global Query Block List, 374
 - domain isolation, 53
 - double encoding, 552
 - EdgeSync traffic, 500
 - Enterprise firewall and Exchange Active Sync Direct Push, 707
 - Exchange 2010 client services, 718
 - Exchange Server 2007, 494
 - Exchange Server 2007 mail filtering, 491
 - Exchange Server 2007 Server Role, 698
 - Exchange Server capacity planning, 705
 - Exchange Setup Logs, 174
 - Exchange Web Services, 723
 - FetchURL, 421
 - file names, matching patterns, 521
 - Firewall Client, migration, 93
 - Forefront Edge Virtual Deployments, 301
 - Forefront Protection 2010 for Exchange Server, 491
 - Forefront Protection Manager 2010, 205
 - Forefront Server Security for Exchange sizing, 523
 - Forefront TMG, migration, 93
 - GAPA (Generic Application-Level Protocol Analyzer), 307
 - hardware requirements, 36
 - HELO/EHLO, 516
 - HRESULT format, 177
 - HTTP 1.1 enhancements, 913
 - HTTP headers, 392, 874
 - HTTP methods, 871
 - HTTP Protocol, 109, 245
 - ICMP messages, 242
 - Internal Certification Authority, 700
 - Internet timeline and milestones, 911
 - IP protocols, 9
 - ISA Data Packager, 892
 - ISA Server, 93, 706
 - ISA Server 2006 Supportability Update, 3
 - ISA Server Common Criteria, 11
 - ISA Server Message Screener, 491
 - Jscript Regular Expressions, 362
 - Kerberos Constrained Delegation, 669–70
 - keyword list, 527

- L2TP over IPsec, 790
- link aggregation, 288
- locallat.txt, 129
- lockouts, 867
- Malware Inspection, 442
- Microsoft Essential Business Server, 4
- name resolution, 59, 259
- NAP planning, 745, 758
- NAT (Network Address Translation), 216
- Netscape, 352
- Network Monitor, 305, 891–92
- network templates, choosing, 32
- Nimda worm, 489
- NLB (Network Load Balancing), 285, 287
- NLB in VMWare ESX Server, 301
- Outlook Anywhere, 704, 718
- Outlook buffer overflow, 489
- Outlook Web Access, troubleshooting, 722
- phishing, 490
- port 6601, 766
- PowerShell, 845–46
- PPTP NAT editors, 734
- PPTP protocol, 788
- quarantine, NAP, 753
- RADIUS, 741, 751
- RAID, 813
- Root DNS Servers, 265–67
- Routing and Remote Access (RRAS), 748
- S4U2Proxy request, 687
- secure hash algorithms, 950
- security by obscurity, 558
- Sender Policy Framework, 218, 515
- SMTP command and response, 512
- spam, 490
- SQL encrypted connections, 811
- SQL Server storage, 815
- SSL version 3, 884
- SSTP, 763, 771, 792
- SVVP (Server Virtualization Validation Program), 25
- TMG Client, 93, 908
- TMG COM methods, 842
- TMG Firewall Log fields, 798–800
- UAG functionality, 28
- virtual deployments, 45
- VLAN, 286
- VPN authentication, 736, 750–51
- VPN connections, 743
- VPN protocols and performance, 741, 774

- Web site publishing rules, 558
- Windows Filtering Platform, 7
- Windows Internet libraries, 969–72
- WinHTTP, 469
- WinINET, 108, 353
- WinINET API, proxy settings, 108
- Winsock Service Providers, 124
- WPAD, 345, 371, 381
- WUA COM API, 322
- WWSAPI, 469
- MRS (Microsoft Reputation Service).
 - See also* URL filtering
 - Bing safe search, 471
 - URL filtering, overview, 465–70
- MS08-067 associated malware, 316–17
- MS-CHAPv2, 736
- MSN Messenger, 562–64
- Multicast, 285–87
- Multicast with IGMP, 285–87
- Multipurpose Internet Mail Extension (MIME), 489
- Music, streaming, 353, 382–84

N

- Name resolution
 - CERN proxy traffic, 246
 - DNS configuration, 289–91
 - migration and, 95
 - Name Service Provider (NSP), 122, 125–32
 - network configurations, 58–63
 - overview, 37–39
 - preinstallation checklist, 141
 - SecureNET clients, 115–17
 - TMGC as name service provider, 125–32
 - troubleshooting, 259
 - Winsock, 119
 - WPAD, configuring, 369
- Name Service Provider (NSP), 122, 125–32
- Name services, 39, 92
- NAP (Network Access Protection)
 - dial-in VPN migration, 91
 - UAG integration, 26
 - VPN integration, 743–45
 - VPN integration, configuring, 756–63
- NAT (Network Address Translation)
 - E-NAT (Enhanced NAT), 265
 - configuring, 820–26

NDIS (network driver interface specification)

- overview, 817–20
- troubleshooting, 826–27
- flood mitigation, 334
- L2TP/IPsec, 735
- network rules, creating, 226–31
- new features, 18–19
- relationships, 215–20
- server publishing rules, 576, 590–91
- web proxy filter, troubleshooting, 532
- NDIS (network driver interface specification), 8
- Negotiate authentications, 878
- NetBIOS, 38, 51, 58–59, 384
- Netmask ordering, 73
- Netscape, 352
- Network Access Protection. *See* NAP (Network Access Protection)
- Network Adaptor properties, 276
- Network Address Translation. *See* NAT (Network Address Translation)
- Network cards, requirements, 35–36
- Network driver interface specification (NDIS), 8
- Network Inspection System (NIS)
 - configuring, 311–16
 - customizing, 316–19
 - flood mitigation, configuring, 330–36
 - IDS and, 322, 326
 - implementing, 309–10
 - intrusion detection, 196–97, 324–26
 - IP preferences, configuring, 327–30
 - logging, 799–800
 - Malware Inspection, 429
 - monitoring, 319–21
 - new features, 17
 - overview, 307–09
 - preconfigured attack protection, 337–40
 - Update Center configuration, 483
 - updates, 322, 478
- Network Interface, counters, 42–43
- Network intrusion, new features, 17
- Network Listener, 589
- Network Listener IP Addresses, 640
- Network Load Balancing (NLB)
 - architecture, 285–88
 - E-Mail Policy Wizard, 498
 - enabling, 288–92
 - migration and, 95
 - publishing rules, 76–80
 - site-to-site VPN connections, 786

- TMG Setup architecture, 171
- traffic flow, 74
- Web server publishing, 606
- Network Load Balancing Integration Wizard, 293
- Network Monitor
 - reading captures, 897–903
 - SharePoint Services, troubleshooting, 693–95
 - SOCKS- proxy troubleshooting, 903–09
 - trace, 371
 - trace, cache information, 418
 - traffic capture, 891–97
- Network Policy and Access Services Server Role, 37
- Network Rule Wizard, 221
- Network Rules, 77
- Network Setup Wizard, 30, 200–02
- Network Template Wizard, 201
- Network Time Protocol (NTP), 590–91
- Network Trace, 419
- Networks
 - 3-Leg Perimeter template, 67–68
 - access, enabling, 22–23
 - Back Firewall template, 68–69
 - bandwidth consumption, 330–36
 - configuring
 - creating networks, 222–31
 - network relationships, 209–22
 - protected networks, 231–39
 - rules, 220–22
 - deploying, virtual environments, 44–45
 - Edge Firewall, 66–67
 - entities, 279–80, 314
 - high availability
 - designing for Access Rules, 80–81
 - for publishing rules, 76–80
 - overview, 71–76
 - infrastructure requirements, 37–41
 - installation, TMG 2010, 162–64
 - installation, TMG MBE, 149
 - ISP Redundancy, 268
 - joining firewall to domain or workgroup, 82–84
 - logging, 798
 - migration, 91–93
 - NAT relationships, 215–20
 - network rules, creating, 220–22, 226–31
 - new features, 18–19
 - NLB considerations, 286–88
 - preinstallation checklist, 141–45
 - protection, UAG, 27–32

- requirements
 - complex networks, 53
 - configuring TMG networks, 54–57
 - name resolution, 58–63
 - TMG deployment options, 51–53
 - traffic profile, determining, 47–51
 - route relationships, 215
 - rules, 241
 - server publishing relationships, 576–77
 - templates, 65–71
 - TMG console, 185, 191, 197–98
 - troubleshooting, 892
 - Web proxy client requirements, 112
 - New Cache Rule Wizards, 401–07
 - New Content Download Job Wizard, 409–12
 - New Network Rule Wizard, 18, 227–31, 822–23
 - New Network Wizard, 224–26
 - New Server Farm Wizard, 681–84
 - New Server Publishing Rule Wizard, 638, 642
 - New SharePoint Publishing Rule Wizard, 672–89
 - New URL Category Set Wizard, 475
 - New Web Listener Wizard, 601, 626–30, 709
 - New Web Publishing Rule Wizard, 604, 631–36
 - Next Generation TCP/IP stack, 12
 - NIC, 268, 288
 - Nimda worm, 489. *See also* Malware protection
 - NIS (Network Inspection System)
 - configuring, 311–16
 - customizing, 316–19
 - flood mitigation, configuring, 330–36
 - IDS and, 322, 326
 - implementing, 309–10
 - intrusion detection, 196–97, 324–26
 - IP preferences, configuring, 327–30
 - logging, 799–800
 - Malware Inspection, 429
 - monitoring, 319–21
 - new features, 17
 - overview, 307–09
 - preconfigured attack protection, 337–40
 - Update Center configuration, 483
 - updates, 322, 478
 - NLB (Network Load Balancing)
 - architecture, 285–88
 - E-Mail Policy Wizard, 498
 - enabling, 288–92
 - migration and, 95
 - publishing rules, 76–80
 - site-to-site VPN connections, 786
 - TMG Setup architecture, 171
 - traffic flow, 74
 - Web server publishing, 606
 - Nmcap.exe, 892, 896
 - nocarp, 949
 - Node types, 58–59
 - Node, JScript, 361
 - Non-HTTP protocols, 78
 - Non-integrated NLB (Network Load Balancing), 288–92
 - Non-TCP/UDP protocols, 117
 - Non-TMG Firewall, 336
 - Non-Windows authentication, 40
 - Normalization, 552
 - nslookup, 371
 - NSP (Name Service Provider), 122, 125–32
 - NTFS partition, 389
 - NTLM authentication, 39–40, 707, 878, 881–82
 - NTP (Network Time Protocol), 590–91
- ## O
- Object Linking and Embedding (OLE), 829
 - OEM (Original Equipment Manufacturers), 21
 - Office SharePoint Services. *See* Microsoft Office SharePoint Services
 - Offline servers, 587
 - OLE (Object Linking and Embedding), 829
 - One-Time Report Wizard, 446–50
 - Operating systems
 - 32-bit, 5, 36–37, 94
 - 64-bit, 5, 11–12, 36–37, 94
 - client selection and, 133
 - migration, 88
 - preinstallation checklist, 141
 - TMG 2010 deployment, 5
 - VPN access, client support, 738
 - OPTIONS, 871
 - Original Equipment Manufacturers (OEM), 21
 - Outbound protocols, publishing, 573
 - Outbound traffic, 22–23, 264, 538–47. *See also* Traffic
 - Outlook, 120, 489–90, 705
 - Outlook Anywhere (OA), 724
 - Outlook Anywhere Publishing, 717–18
 - Outlook Anywhere Services, 77, 705, 707
 - Outlook Express, 489

Outlook Mobile Access, 704, 707
Outlook Web Access (OWA), 16, 76–78, 587, 698–702,
704, 709–17, 721–23
Ownership relationships, 96–99

P

Packets, 9–10, 50, 938
Partitions, 35–36, 389
Passive caching, 920
Password Authentication Protocol (PAP), 735
Passwords, 235
Path mismatch, 651
Payload length, 552
Peer node type (PNode), 59
Performance. *See also* Behavioral monitoring;
Load balancing
authentication, 39–40
cache, 394–95, 421–22
CARP (Cache Array Routing Protocol), 395–97
counters
cache, 395, 939
compression performance, 953
DiffServ, 954
e-mail hygiene, 960
Firewall packet engine, 938
H.323 filter, 939
how to use, 964
HTTPS performance, 959
malware protection, 956
Microsoft Firewall service, 941
overview, 937–38
requirements, 41
SOCKS filter, 943
TMG Performance Monitor, 962
URL filtering, 961
Web proxy, 944
Exchange Server, 705–06
logging options, 811
Malware Inspection, 437–39
migration, 94
monitoring, requirements, 41–43
name resolution, 37–39, 62, 246
networks, requirements, 42–43
preinstallation checklist, 143–45
proxy cache, 387–89
proxy redundancy, 380
System Performance, 964
virtual environments, deploying in, 44–45
Virus Filtering, 523
VPN access, 739
Performance Monitor, 58, 861, 962
Perimeter networks, 223
Persistent connection, 916
Phishing, 469, 487–90
PICNIC, 88
Ping of death, 325
Ping requests, 212–15, 242–45
ping.exe, 125–26
Pipelined requests, 913
PKI (Public Key Infrastructure), 593
PNode (peer node type), 59
Point-to-Point Tunneling (PPTP)
access, enabling, 22–23
over HTTP, 735
overview, 734
protocol mapping, 50
site-to-site VPN connections, 773–74,
782–88
technology comparison, 736–37
TMG deployment options, 52–53
troubleshooting VPN connections, 788–90, 793
Policies. *See also* Access control; Filtering
Active Directory Lightweight Directory Services
(LDS), 147
Additional Security Policy, 188
arrays, 299, 837
authentication, 39–40
CERN proxy HTTP traffic, 242–49
E-mail Policy, 194–95, 205
firewall policy, 188, 194
HTTP policy, 581
migration and, 87
name resolution, 37–39
ping requests, 242–45
Policy Enforcement, 249–53
Policy Reevaluation, 249–53
Protocol Anomalies, 315
server publishing, 574–76
system policy, 172
TMG deployment options, 52–53
traffic, 7, 241–49
troubleshooting access rules, 253–62
UAG, 26
URL filtering, new features, 16

- VPN (Virtual Private Networks), 733–36, 741–42
 - Web Access Policy, 188–90, 194, 562–64, 568
- Policy engine, rule basics, 241–49
- Polling, 265–66, 481
- POP Intrusion Detection, 326
- POP3 Intrusion Detection filter, 590
- Pornographic content, 471
- Portal trunks, 24
- Ports
 - firewall rules, 24
 - HTTP, 870
 - HTTP.SYS, 763
 - logging, SQL listeners, 806
 - non-Web servers, 642–47
 - PPTP, port 1723, 734, 788–90
 - protocol mapping, 50–51
 - redirect requests, 617
 - redirection, 583–84
 - server publishing, 590–91
 - SharePoint Services, 690
 - source port affinity, 72
 - SSTP, 766
 - TCP port 80, 900
 - UAG, security and, 26
 - Web listener, 580
- POST, 871, 913
- Post Office Protocol (POP), 326, 590
- PowerShell, 171, 842–48
- PPTP (Point-to-Point Tunneling)
 - access, enabling, 22–23
 - overview, 734
 - protocol mapping, 50
 - site-to-site VPN connections, 773–74, 782–88
 - technology comparison, 736–37
 - TMG deployment options, 52–53
 - troubleshooting VPN connections, 788–90, 793
- PrerequisiteInstaller.DATE-TIME.log, 175
- Printer Sharing, 144
- Private keys, 91, 662
- Processors, 5, 35–37, 94, 523
- Productivity, new features, 16. *See also* Performance
- Protected networks, Access Rules, 80–82. *See also* Access control
- Protocol Anomalies Policy, 315
- Protocol filters, 308
- Protocols
 - client selection, 133
- HTTP
 - anonymous requests, 877
 - authentication delegation, 883
 - authentication methods, 878
 - dual authentication (proxy and server), 881
 - More Info, 109
 - NTLM authentication, 881–82
 - overview, 869–74, 911–17
 - proxy authentication, 879–80
 - server authentication, 878–79
- HTTPS, overview, 884–89
 - mapping, 50–51
 - non-TCP/UDP, 117
 - Point-to-Point Tunneling (PPTP), 734
 - publishing consideration, 593–95
 - redirection, 583–84
 - server publishing, 78, 589
 - SMTP (Simple Mail Transfer Protocol), 47–51
 - SSTP, 23
 - TMG deployment options, 52–53
 - tunneling, 22–23
 - Web Listener, 77
- Proxy authentication, 875–76, 879–80
- Proxy cache, overview, 387–89
- Proxy chaining, 922
- Proxy Server, history of, 923–35
- Proxy servers
 - overview, 918–23
 - public, 534–38
 - WPAD (Web Proxy Auto Discovery), 353
- Proxy sorting, 361
- Proxy traffic, migration and, 94
- Proxy, migration, 92–93
- ProxyEnable, 108
- ProxyOverride, 108
- ProxyServer, 108
- Public Key Infrastructure (PKI), 593, 703
- Publishing
 - availability, rules, 76–80, 216, 218
 - Exchange Server
 - configuring, 707–18
 - planning for, 697–707
 - troubleshooting, 719–30
 - migration, 90–91, 94
 - non-Web servers, 637–47
 - planning rules, 591–97
 - published servers, 117
 - scenarios, 573–80

- server publishing, 574–77, 588–91
- servers, troubleshooting, 647–56
- SharePoint Services
 - configuring, multi-server, 672–79
 - configuring, overview, 665–66
 - configuring, server farm, 679–89
 - configuring, single-server, 667–72
 - planning for, 661–65
 - troubleshooting, 689–95
- SMTP, configuring, 820–26
- Test Button, 656–57
- troubleshooting, 657–60
- Web publishing, 578–88
- Web servers
 - HTTP, 600–18
 - HTTP protocol, 600–18
 - HTTPS, 599–636
 - overview, 599–600
- Web site publishing rules, creating, 558
- PUT, 871, 913

Q

- Quarantined VPN clients, 31, 91, 223, 753
- Query Length, 552
- querystring, 405
- Queues, 24, 42, 809, 814

R

- RADIUS, 40, 237–38, 663–64, 741, 751, 762–63
- Radius Server Settings, Configure, 190
- RAID hardware mirroring, 35, 812–13
- RAM
 - caching, 389–91
 - flood mitigation, 330–36
 - hardware requirements, 35–36
 - log files, 803–04, 812–13
 - TMG requirements, 12
 - VPN access, requirements, 740–41
- RDP client, 353
- Reading, log files, 176
- Receive Auto Tuning, 12
- Recipient Filtering, 512–13
- Recurring Report Job Wizard, 451–55
- recv, 121

- Redirect requests, 617
- Redundancy
 - Enable ISP Redundancy Wizard, 206
 - hardware requirements, 35–36
 - ISP Redundancy, 78–79, 263–65
 - UAG, security and, 26
- Registry, 481
 - WinINet updates, 108
- Reliability
 - best practices, 298–99
 - configuring, 293–98
 - enabling, 288–92
 - ISP redundancy, 263–65, 267–84
 - ISP Redundancy Configuration Wizard, 269–74, 276–84
 - ISPRedundancyConfig, 266
 - link availability testing, 265–67
 - NLB architecture, 285–88
 - rule basics, 242
 - TMG console, 197–98
 - troubleshooting, 301–06
 - virtual environments, 300–01
- Remote access
 - hardware requirements, 36
 - management, 147, 172–74, 299
 - protocol mapping, 51
 - single-NIC, 31
 - TMG console, 192
 - TMG deployment options, 52–53
 - TMGC, Winsock requests, 129
 - UAG, security, 26
 - VPN
 - dial-in clients, 747–56
 - L2TP over IPsec, configuring, 774–81
 - NAP integration, 743–45
 - NAP integration, configuring, 756–63
 - overview, 733–36
 - planning access, 737–43
 - site-to-site, 773–74, 782–93
 - SSTP configuration, 763–71
 - technology comparisons, 736–37
- Remote Authentication Dial-In User Service (RADIUS), 40, 237–38, 663–64, 741, 751, 762–63
- Remote Desktop
 - installation, TMG 2010, 165
 - installation, TMG MBE, 152
- Remote Procedure Call (RPC), 47–51, 77, 120, 590, 704

Report Generation Warning, 800

Reporting

Active Directory Lightweight Directory Services (LDS), 147

cache behavior, 417–20

IIS, default links, 37

logging options, 800–03

Malware Inspection, 429–30, 446–63

new features, 14–16

TMG console, 192–93

Reputation Service. *See* Microsoft Reputation Service (MRS)

REQUEST fields, 871

Require All Users To Authenticate, 238–39

Requirements

client selection, 134

deploying in virtual environments, 44–45

hardware, 35–36

network infrastructure, 37–41

complex networks, 53

configuring TMG networks, 54–57

name resolution, 58–63

TMG deployment options, 51–53

traffic profile, determining, 47–51

performance monitoring, 41–43

SecureNET clients, 113–14

software, 36–37

Web proxy clients, 112

Resource consumption, flood mitigation, 330–36

Reverse caching, 391, 394–95, 920

Reverse proxy, 921–22

Reverse-lookups, 38–39, 516

Rolling upgrades, 88

Root Certification Authority, new features, 16

Root DNS servers, 265–67

Routing. *See also* CARP (Cache Array Routing Protocol)

IP routing, basic, 210–15

network structure, migrating, 91

networks rules, creating, 226–31

route relationships, 215

source routing, 329

split routing infrastructure, 48

Routing and Remote Access Service (RRAS), 171, 748, 763

RPC (Remote Procedure Call), 47–51, 77, 120, 590, 704

RTSP, 50, 382–84

Rule-based URL filtering, configuring, 475–76

S

S4U2Proxy requests, 687

Safe list services, 503–05

Safe Search, Bing, 471

SANs (Subject Alternate Names), 662

Scenarios

caching, 390–91

migration, 90–95

publishing, 573–80

Schedules, 96, 582, 663

SCL (Spam Confidence Level), 511–12

Scripting

best practices, 834–36

JScript

importing and exporting files, 838

JScript Regular Expressions, 362

locating arrays, 837

objects, 357–59, 361

overview, 834

WPAD, cfile, 352–64

task automation, 836–42, 845–48

TMG Component Object Model (COM), 829–34

VBScript

importing and exporting files, 838

locating arrays, 837

overview, 834

PowerShell conversions, 846

save changes, 841

Windows PowerShell, 37, 171, 842–48

WPAD script CARP operation, 947–54

Search, Bing, 471

Secure Socket Tunneling Protocol (SSTP)

configuring, 763–71

overview, 735

TMG deployment options, 52–53

troubleshooting, 771, 792–93

VPN protocol, 23, 736–37

Secure Sockets Layer (SSL)

authentication, protected networks, 237

cache rules, 392

connection requests, 110

Exchange Server, 699–700, 703–04

handshake, 703, 884

HTTPS, overview, 884–89

new features, 16

SharePoint Services, 662, 665

SSL-ID affinity, 73–75

- tunnels, ports for, 111
- web proxy client calls, 534
- SecureNET clients
 - authentication, 239
 - client considerations, 293
 - features of, 135
 - firewall chaining, 335
 - migration, 93
 - overview, 113–18
 - traffic management, 81–82
- SecureNETSecureNET, 70
- SecurID, 664
- Security
 - client selection and, 133–34
 - logging, importance of, 797–98
 - preinstallation checklist, 141
 - SharePoint Services, 661–63
 - site-to-site VPN connections, 774
 - UAG, aligning, 26
 - updates, 173–74
 - URL filtering, new features, 16
 - virtual environments, deploying in, 45
 - VPN access, 738–39
- Security Alert, 15
- Security by obscurity, 558
- send, 121
- Sender Filtering, 513–15
- Sender ID, 515–16
- Sender open proxy test, 517
- Sender Policy Framework (SPF), 218, 515–16
- Sender Reputation Level (SRL), 515–18
- SendLogonOn401, 702
- Server Acknowledgement, 889
- Server Certificate errors, 549
- Server Connection Security, 606
- Server farms, 587–88, 606, 679–89
- Server hello, 886
- Server Key Exchange, 887
- Server Message Block (SMB), 51
- Server publishing
 - access rules and, 577
 - network relationships and, 576–77
 - non-Web, 78, 637–47
 - overview, 574–76
 - rule, 588–91
 - Single NIC firewalls, 70
- Server Virtualization Validation Program (SVVP), 25
- ServerManagerCmdInstallLogDATE-TIME, 175
- Servers, dedicated servers list, 278, 282
- Server-side CARP, 397
- Server-side configurations, Web proxy, 111
- Service packs, TMG Setup options, 173–74
- Service Principal Name, 669, 677
- Service Provider Interface (SPI), 122–25
- Session Affinity, 587
- Session ID, 885
- Session Initiation Protocol (SIP) filter, 18, 50, 205, 336, 590
- Settings
 - authentication, Web listener, 602–03
 - cache, 397–400, 407–12
 - flood mitigation, 339–40
 - Intrusion Detection System (IDS), 324
 - Malware Inspection, 437–38
 - NIC configuration, 268
- Setup, TMG
 - architecture, 169–72
 - options, 172–74
 - troubleshooting, 174
- Sharepoint, 587
- SharePoint Services
 - configuring
 - multi-server, 672–79
 - overview, 665–66
 - server farm, 679–89
 - single-server, 667–72
 - publishing, planning for, 661–65
 - troubleshooting, 689–95
- SharePoint Web Publishing Wizard, 665–72
- shExpMatch(), 949
- Signatures
 - HTTP Filter, 561–70
 - new features, 13
 - NIS (Network Inspection System)
 - configuring, 311–16
 - implementing, 309–10
 - IP preferences, configuring, 327–30
 - monitoring, 319–21
 - overview, 308–09
 - updates, 322
 - Update Center, 478–81
- Simple Mail Transfer Protocol. *See* SMTP (Simple Mail Transfer Protocol)
- Simplex, 78
- Single network adapter, 52–53, 223
- Single NIC, 62, 69–71

- Single-NIC, 31–32
- Single-Sign-On (SSO), 580
- SIP (Session Initiation Protocol) filter, 18, 50, 205, 336, 590
- SirCam virus, 488–90
- Site-to-site (S2S) VPN
 - migration, 92
 - Network Inspection System (NIS), 336
 - overview, 773–74
 - PPTP, configuring, 782–88
 - troubleshooting connections, 788–93
- skiphost, 949, 952
- Smart-card authentication, 719–20
- SMB (Server Message Block), 51
- SMTP (Simple Mail Transfer Protocol)
 - configuring, 493–501, 518–27
 - E-Mail Protection Wizard, 494–501
 - Enhanced NAT (E-NAT), 817–20
 - new features, 16–17
 - protection, overview, 490–92
 - publishing rules, 658–60
 - route relationships, 215
 - server publishing, 590
 - SMTP Message Screener, 490–91
 - SMTP Protection, 174
 - SMTP Publishing, configuring, 820–26
 - spam filtering, configuring, 502–18
 - traffic profile, 47–51
- socket, 121
- SOCKS filter, 937, 943
- SOCKS-proxy, troubleshooting, 903–09
- Software requirements, 36–37, 88
- Source IP affinity, 72, 74–75
- Source port affinity, 72
- Source routing, 329
- Spam
 - e-mail threats, overview, 487–90
 - Exchange (Anti Spam), 479
 - filtering, configuring, 502–18
 - new features, 16–18
 - overview, 490
 - policies, 194–95
- Spam Confidence Level (SCL), 511–12
- spash.hta, 171
- SPF (Sender Policy Framework), 218, 515–16
- SPI (Service Provider Interface), 122–25
- Spindle, 429
- Split routing infrastructure, 48
- SPNEGO, 878
- Spoof detection, 337–38
- Spyware. *See* Malware protection
- SQL Express, 804–05
- SQL Server 2008, 171, 802–07
- SQL Server Express Database, 802
- SQL Server Reporting Services (SRS), 14–16
- SQL Server, best practices, 815
- SRL (Sender Reputation Level), 515–18
- SSL (Secure Sockets Layer)
 - authentication, protected networks, 237
 - cache rules, 392
 - connection requests, 110
 - Exchange Server, 699–700, 703–04
 - HTTPS, overview, 884–89
 - new features, 16
 - SharePoint Services, 662, 665
 - SSL-ID affinity, 73–75
 - tunnels, ports for, 111
 - web proxy client calls, 534
- SSL (Secure Sockets Layer) handshake, 703, 884
- SSO (Single-Sign-On), 580
- SSTP (Secure Socket Tunneling Protocol)
 - configuring, 763–71
 - overview, 735
 - TMG deployment options, 52–53
 - troubleshooting, 771, 792–93
 - VPN protocol, 23, 736–37
- Stateful failover, 264
- Stateful inspection, 10
- Static Proxy, 81–82
- Status codes, 873, 914
- Storage, 389, 395, 439–40, 803–04, 812–13.
 - See also* Memory
- Streaming media, 50, 330, 353, 382–84, 590
- Strict Source Routing, 329
- Stripe sets with parity, 813
- Subject Alternate Names (SANs), 662
- SuccessesToAvailable, 267
- Supportability, VPN access, 742
- SVCHOST.EXE (Windows Server service), 567
- SVVP (Server Virtualization Validation Program), 25
- Switch flooding, 286–87
- Symmetric bridging, 584
- SYN attack protection, 337–40
- System Center Operations Manager, 44
- System Configuration Wizard, 200, 202

System node, TMG console, 191
System Performance, 964
System policy, 172

T

Task automation, 836–42
TCP 3-way handshake, 870
TCP 4-way closing handshake, 870
TCP connections
 attacks against, 323
 flood mitigation, 330–36
 non-Web servers, 637–47
 port 1723, PPTP, 734
 ports
 135, 50
 1743, 117
 443 (HTTPS), 28, 111
 593, 111
 80, 15
 8008, 15, 37
 8080, 109
 route relationships, 215
 source port affinity, 72
 PPTP, port 1723, 788–90
 SharePoint Services, 690
 WPAD, Internet Explorer configuration, 376
TCP handshake, 884
TCP sequence protection, 338–40
Teardrop attack, 329
Templates
 3-Leg Perimeter, 67–68
 Back Firewall, 68–69
 Edge Firewall, 66–67
 Single NIC firewall, 69–71
Terminal Services Gateway, 73, 77
Test Rule, 612, 725–30
Testing. *See also* Troubleshooting
 ISP-Redundancy, 265
 Test Button, Web publishing, 656–57
 URL filtering, 476
TestIntervalLinkAvailable, 267
TestIntervalLinkUnavailable, 267
Text logs, 807–08
TFTP (Trivial File Transfer Protocol) Filter, 18, 50
Third-party platforms, 301
Third-party solutions, high-availability, 74, 76
Timeout values, HTTP(S) connections, 706–07, 721
Time-To-Live (TTL), 78–79, 95, 392
TMCG Control Channel, 127
TMG. *See* Microsoft Forefront Threat Management Gateway (TMG)
TMG MBE. *See* Microsoft Forefront Threat Management Gateway (TMG), Medium Business Edition (MBE)
tmgbook.hash.and.sort.js, 947–48
TRACE, 871
Traffic. *See also* Network Inspection System (NIS)
 buffering, requirements, 37–41
 captures, Network Monitor, 891–97
 captures, reading captures, 897–903
 CERN proxy HTTP, 242–49
 control, requirements, 40–41
 Exchange Server, performance, 703–06
 filtering, 6–8, 22–23
 ISP Redundancy, 268
 load, authentication, 40
 NAT relationships, 215–20
 network design
 availability, for publishing rules, 76–80
 availability, overview, 71–76
 for Access Rules, 80–81
 protected networks, 231–39
 network relationships, overview, 209–22
 network rules, creating, 226–31
 ping requests, 242–45
 policy behavior, 241–49
 Policy Reevaluation, 249–53
 profile, determining, 47–51
 proxy traffic, migration and, 94
 route relationships, 215
 TMG Setup options, 172–74
 troubleshooting access rules, 253–62
Traffic Simulator, 259–62, 859
Transactions, HTTP, 870–74
Transparent proxy requests, 649–50
Transport mode, VPN tunnels, 734
Transport Service Provider (TSP), 122, 125–32
Trickling, 431, 438–39
Trihomed perimeter network, 30
Trivial File Transfer Protocol (TFTP) Filter, 18, 50
Troubleshooting. *See also* Performance, counters
 access rules, 253–62
 availability, 80
 Best Practices Analyzer (BPA), 860–61
 cache, 417–23

- case study, 862–68
- client types, 136
- Enhanced NAT (E-NAT), 826–27
- Exchange Server, 719–30
- general methodology, 851–55
- Internet Explorer and WPAD, 381
- load balancing, 286, 301–06
- logging, 798–800
- Network Monitor
 - overview, 861
 - reading captures, 897–903
 - SOCKS-proxy, 903–09
 - traffic capture, 891–97
- Performance Monitor, 861
- PICNIC, 88
- publishing rules, 647–56
- SharePoint Services, 689–95
- SSTP connectivity, 771
- tab, Management Console, 858–59
- TMG console, 186
- TMG Setup
 - architecture, 169–72
 - failure of, 174
 - setup options, 172–74
- tools for, 855–58
- VPN client connections, 788–93
- web proxy traffic, 532
- Windows Event Logs, 862
- Trunks, types, 24
- Trust, HTTP, 874–83
- Trusted Root certificate store, 535
- TSP (Transport Service Provider), 122
- TTL (Time-To-Live), 78–79, 392
- Tunnel-based publishing, 588–91
- Tunneling protocols, 22–23
- Tunnels, VPNs
 - dial-in clients, configuring, 747–56
 - NAP integration, 743–45
 - NAP integration, configuring, 756–63
 - overview, 733–36
 - planning access, 737–43
 - site-to-site
 - L2TP over IPsec, configuring, 774–81
 - overview, 773–74
 - PPTP, configuring, 782–88
 - troubleshooting, 788–93
 - SSTP configuration, 763–71
 - technology comparisons, 736–37

U

- UAG. *See* Unified Access Gateway (UAG)
- UDP. *See* User Datagram Protocol (UDP)
- Unattended installations, TMG, 168, 171–72
- Unicast, 285–86
- Unified Access Gateway (UAG)
 - access, enabling, 22–23
 - deployment, 27–28
 - future release, 21
 - IAG 2007, 23–24
 - ISA Server, 24
 - network protection, designing, 27–32
 - new features, 25–26
 - security needs, aligning, 26
- Unified Messaging Server, 698
- Uniform Resource Identifier (URI), 912
- Unihomed network, 31–32
- Update Center. *See also* Updates
 - configuring, 481–85
 - Medium Business Edition (MBE), 185
 - NIS (Network Inspection System), 322
 - overview, 199, 478–81
 - TMG console, 187
- Update Configuration, 440
- Updates. *See also* Update Center
 - dynamic update, 370–74
 - hotfix, Hyper-V, 301
 - migration, preparation for, 88
 - NIS (Network Inspection System), 315, 322
 - TMG console, 192–93
 - TMG Setup options, 173–74
- Upgrades, rolling, 88
- URI (Uniform Resource Identifier), 912
- URL correction, 664–65
- URL filtering
 - category overrides, 477–78
 - configuring, 470–78
 - HTTP Filter, 533–34
 - manual, 429
 - maximum URL length, 552
 - overview, 465–70
 - performance counter, 938, 961
 - TMG Setup architecture, 171
 - TMG, new features, 15–16, 194
 - Update Center, 478–81
 - configuring, 481–85
- URL Filtering Updates, 479

URLs

- CARP (Cache Array Routing Protocol), 395–97
- ConvertUrlToLowerCase, 355–56
- FetchURL, 421

- User Agent, HTTP, 916

User Datagram Protocol (UDP)

- bidirectional protocols, 574
- flood mitigation, 334
- non-Web servers, 637–47
- route relationships, 215
- source port affinity, 72
- UDP bomb alert, 326
- UDP port 1701, 735
- UDP port 500, 735

- User Groups, 663

- User interface, new features, 14–16

Users

- authentication, WDigest, 235
- Exchange Server planning, 705
- IIS requests, 24
- logging, 797
- mobile, 27
- Require All Users To Authenticate, 238–39
- Web proxy client, 354
- Web publishing rules, 610
- Web server rules, 635

V

Validation

- HTTP Filter, 550, 564–67
- HTTPS Inspection, 538–47
- requirements, 39–40
- Server Virtualization Validation Program (SVVP), 25
- SharePoint Services, 663–64
- Test Rule, publishing, 612

- Variants, URL, 468

VBScript, 834

- importing and exporting files, 838
- locating arrays, 837
- PowerShell conversions, 846
- save changes, 841

- verbose mode, 176

- Version control, 315

- Video streams, 18, 382–84

- VIP (Virtual IP addresses), 285, 290, 498, 606

- Virtual environments

- deployment requirements, 44–45

- hardware requirements, 36

- load balancing, 300–01

- TMG deployment options, 52–53

- UAG deployment, 25

- Virtual IP addresses (VIPs), 285, 290, 498, 606

Virtual Private Networks (VPN)

- access, enabling, 22–23

- creating, 222–24

- dial-in clients

- configuring, 747–56

- migration, 91–92

- NAP integration, 756–65

- overview, 733–36

- planning access, 737–43

- quarantined clients, 31

- Single NIC firewalls, 69–70

- site-to-site

- L2TP over IPsec, configuring, 774–81

- overview, 773–74

- PPTP, configuring, 782–88

- troubleshooting, 788–93

- SSTP configuration, 763–71

- technology comparisons, 736–37

- TMGC, Winsock requests, 129

- VPN Clients Network, 222–24

- Virus Filtering, 522–25

Virus protection

- AnnaKournikova, 488–89

- BadTrans, 489–90

- BubbleBoy, 489–90

- configuring, 518–27

- e-mail threats, overview, 487–90

- ILOVEYOU, 488–89

Malware Inspection

- content delivery, 438–39

- environment considerations, 431–36

- Internet access, testing, 443–45

- overview, 427–31

- per-rule, defining, 442

- reports, creating, 446–63

- settings, configuring, 437–38

- storage, 439–40

- Update Configuration, 440

- Melissa, 488–89

- new features, 11–14

- SirCam, 488–89

- Update Center, 478–81

VLAN, 286
 VLAN tagging, 288
 VMWare, 301
 VMWare ESX Server, 301
 Voice Over IP (VoIP)
 Configure SIP Wizard, 205
 route relationships, 215
 TMG, new features, 18
 VPN Clients Network, 222–24
 VPNs. *See* Virtual Private Networks (VPN)

W

WAN (wide area networks), 48, 592–93, 773
 Waveform audio format (.wav), 489
 WDigest, 235
 Web Access Policy, 185, 188–90, 194, 562–64, 568
 Web Access Policy Wizard, 200, 203, 431, 536
 Web Access Wizard, 16, 473
 Web Antivirus, new features, 11–14
 Web caching, 36, 69–70
 Web chaining, 77, 91, 93, 242, 335
 Web client requests, 650
 Web farms, load-balancing, 26
 Web filters, 191, 578–80. *See also* Malware Inspection
 Web Listener Wizard, 768–69
 Web listeners, 77, 91, 618, 625–30, 653–54, 766
 Web objects, caching, 392
 Web Proxy
 cache, overview, 387–89
 clients
 availability, 81–82
 cfile, 354
 features of, 135
 NLB, 293
 overview, 107–13
 preinstallation checklist, 142
 with TMGC, 132
 logging options, 800–03
 performance counters, 937, 944
 requests, authentication, 103
 requests, troubleshooting, 649–50
 servers
 authentication, 40
 availability, 80–81
 hardware requirements, 36
 Single NIC firewalls, 69–70
 TMG deployment options, 52–53
 SSTP protocol, 735
 Web Proxy Automatic Discovery (WPAD)
 client applications
 Automatic Proxy Cache, 379–80
 AutoProxy in managed code, 384–85
 Internet Explorer, configuring, 375–79
 overview, 374
 TMG Client, 381–82
 Windows Media Player, 382–84
 configuring, 364–74
 overview, 968
 protocol, 345–52
 script, 352–64
 script CARP operation, 947–54
 troubleshooting, Internet Explorer, 381
 Web Proxy Filter, 265, 429, 573, 580
 Web Proxy Log, 469
 Web Publishing. *See also* Microsoft Office SharePoint Services
 NAT relationships, 218
 network design for, 76–78
 overview, 578–80
 rules, 91, 580–88
 SharePoint Services, 662
 Test Button, 656–57
 troubleshooting, 647–56
 Web Publishing Load Balancing (WPLB), 72, 78–80
 Web Server (IIS) Server Role, 37
 Web servers
 HTTP protocol, 600–18
 HTTPS protocol, 618–36
 publishing, overview, 599–600
 server farm, 587–88
 Web site publishing rules, 558
 Web-based applications, mapping, 49
 Web-based e-mail, new features, 16, 24. *See also* E-mail
 WebRequest, 108
 Welcome Screen, TMG MBE, 185–86
 WFP (Windows Filtering Platform), 6–7
 Whale, 24
 Whiteboards, 18
 Wide area networks (WAN), 48, 592–93, 773
 Windows 2000, 374
 Windows 2003, 374
 Windows 2004, 374
 Windows authentication, 39–40, 663–64, 806
 Windows Automatic Updates, 479–81

- Windows Crypto API (CAPI), 535
- Windows DHCP Client API, 346
- Windows DNS resolver, 63
- Windows Essential Business Server (EBS), 11–12
- Windows Event Logs, 862. *See also* Logging
- Windows Executable Content, 552
- Windows Filtering Platform (WFP), 6–7
- Windows Firewall, traffic policies, 7
- Windows Internet Connection Firewall (ICF), 7
- Windows Internet Libraries, 967
- Windows Internet Name Service (WINS), 58–59
- Windows Media Player, 353, 382–84
- Windows Out-of-Band (WinNuke), 325
- Windows Performance Monitor. *See* Performance Monitor
- Windows PowerShell, 37, 171, 842–48
- Windows Security Support (SSP), 235–36
- Windows Server 2003, 7, 94, 287, 690
- Windows Server 2008, 5, 11–12, 36, 94, 370–74, 739, 763
- Windows Server 2008 Hyper-V RTM, 301
- Windows Server service (SVCHOST.EXE), 567
- Windows Server Update Services (WSUS), 479–81, 484
- Windows Sockets. *See* Winsock
- Windows Temp folder, 174
- Windows Update Agent (WUA) API, 322
- Windows Web Services API (WWSAPI), 469
- Windows XP, 374
- WinHTTP, 353, 384–85, 469, 967–72
- WinHTTP API, 107
- WinHttpGetProxyForUrl, 384
- WinInet, 969
- WinINet, 108, 353, 967
- WinNuke, 325
- WINS (Windows Internet Name Service), 38, 58–59, 92–93
- Winsock
 - logging, 798–99
 - overview, 119–22
 - providers, 122–25
 - TMGC as layered service provider, 125–32
 - Web proxy clients, 113
- Wizards
 - Certificate Import Wizard, 621–25
 - Configure E-mail Policy Wizard, 205
 - Configure SIP Wizard, 205
 - Configure Web Access Policy Wizard, 397–400
 - Connect to Forefront Protection Manager 2010 Wizard, 204–05
 - Create VPN Site-To-Site Connection Wizard, 775–80, 782–87
 - Deployment Wizard, 200, 202–03
 - E-Mail Policy Wizard, 495–501
 - E-Mail Protection Wizard, 494–501
 - Enable ISP Redundancy Wizard, 206
 - Exchange Publishing Wizard, 698–700
 - Exchange Server, 702–03
 - Getting Started Wizard, 54–57, 66–67, 69–70, 174, 200–01
 - ISP Redundancy Configuration Wizard, 269–74, 276–84
 - Join Array and Disjoin Array, 203–04
 - Network Load Balancing Integration Wizard, 293
 - Network Rule Wizard, 221
 - Network Setup Wizard, 30, 200–02
 - New Cache Rule Wizards, 401–07
 - New Content Download Job Wizard, 409–12
 - New Network Rule Wizard, 18, 227–31, 822–23
 - New Network Wizard, 224–26
 - New Server Farm Wizard, 681–84
 - New Server Publishing Rule Wizard, 638, 642
 - New SharePoint Publishing Rule Wizard, 672–89
 - New URL Category Set Wizard, 475
 - New Web Listener Wizard, 601, 709
 - New Web Publishing Rule Wizard, 604
 - new, overview, 199–200
 - One-Time Report Wizard, 446–50
 - Recurring Report Job Wizard, 451–55
 - SharePoint Web Publishing Wizard, 665–72
 - System Configuration Wizard, 200, 202
 - TMG Installation Wizard, 147, 152, 160, 170
 - Web Access Policy Wizard, 200, 203, 536
 - Web Access Wizard, 16, 473
 - Web Listener Wizard, 768–69
- WLBS display, 305–06
- WLBS IP2MAC, 305
- WLBS query, 304
- wlbs.exe, 304–06
- Workgroups, 60–61, 82–84, 94
- Worms. *See also* Malware protection
 - BadTrans, 490
 - Conficker, 567–70
 - e-mail threats, overview, 487–90
 - flood mitigation, 333

- intrusion detection, 323
- KaK, 489–90
- Update Center, 478–81
- WPAD (Web Proxy Automatic Discovery), 968
 - client applications
 - Automatic Proxy Cache, 379–80
 - AutoProxy in managed code, 384–85
 - Internet Explorer, configuring, 375–79
 - overview, 374
 - TMG Client, 381–82
 - Windows Media Player, 382–84
 - configuring, 364–74
 - migration, 93
 - protocol, 345–52
 - script, 352–64
 - script CARP operation, 947–54
 - troubleshooting, Internet Explorer, 381
- wpad queries, 371
- wpad.dat, 375
- WPLB (Web Publishing Load Balancing), 72, 78–80
- Write conflicts, 389
- wspad.dat, 126, 128
- wspsrv.exe, 469
- WSUS (Windows Server Update Services), 479–81, 484
- WWSAPI (Windows Web Services API), 469
- WWW-Authenticate, 875

About the Authors

The guys that wrote this book spent a year working together on this one project. What follows offers some insight into how they were able to tolerate each other for so long.

About Jim Harrison



I'm a retired U.S. Navy ET1(SW) who spent my Navy time on three ships: the U.S.S. Proteus (AS-19), the U.S.S. Nimitz (CVN-68), and the U.S.S. California (CGN-36) as well as NAS Corpus Christi, Texas, Naval Station San Diego, and Naval Station Bremerton, Washington. It was during this time that I learned the fine art of complex system troubleshooting on various radar, radio, GPS, depth-finding, and computer equipment.

I began working at Microsoft in 1999 as a Volt contractor in the Windows Media division, helping to create a product called Digital Broadcast Manager (DBM). I joined Microsoft full-time in 2000. Later that year, I moved to the NetDocs team as a network deployment tester. During this time, I was encouraged to familiarize myself with ISA Server 2000. As they say, the rest is history.

I joined the ISA SE team in 2003 as a test engineer helping to test and ship updates and managing customer cases escalated from CSS to the product team. I present on ISA Server and TMG twice a year at Tech Ed US and Black Hat LV. I also enjoy writing a few ISA blogs, answering the rare forum posting, and producing an occasional Tales from the Edge article.

I fill my copious spare time with my wife and two cats, wandering in the woodlands of western Washington, playing guitar, woodworking, and general home handyman activities (OK—honey-dos). When I get the chance, I run around the backyard with my two-year-old grandson until he wears me out.

About Yuri Diogenes



I started working in the IT field as a computer operator back in 1993 using MS-DOS and Windows 3.1. In 1998 I moved to a Microsoft partner and worked as an instructor for computer classes; I also wrote internal training materials such as NT 4 and Networking. In 1999 I moved to another Microsoft partner as part of a team responsible for maintaining the network of a major Brazilian telecommunications company. There I was responsible for administering the core servers running NT 4.

In December 2003, I moved to the United States to work for Microsoft as a Comptech contractor in the CSS for the Latin America messaging division, where I supported Exchange. In 2004 I moved to Dell Computers in Round Rock, Texas, to initially work as Server Advisor in the Network Operating System Team, dealing primarily with Windows, Exchange, and ISA. I came back to Microsoft as a full-time employee in 2006 to work again on CSS for LATAM, but this time I was focused on the platform division (Networking and ISA Server).

I joined the CSS ISA Team in 2007 as a Security Support Engineer and started to be fully dedicated to ISA. In 2008 my friend Nathan Bigman had the idea to create the Tales from the Edge. Jim Harrison and I started leading this project; eventually many other engineers started to contribute as well. In 2009 I became Senior Security Support Escalation Engineer on the ISA Team, which gave me some new responsibilities.

I like to spend my spare time with my wife, Aleksandra, and my two daughters, Yanne and Ysis. We enjoy traveling, watching movies, and playing on our Xbox 360.

About Mohit Saxena



Right after my graduation from college in 2002, I started working for Dell computers in New Delhi. The whole concept of phone support was new to me and I believe this is where I learned the basics of troubleshooting and customer handling. After spending a year with Dell I moved to Convergys India Services, where I joined the Microsoft Enterprise Platform Support on the Networking Team. In 2004, when the Enterprise Platform Support teams were being formed at Microsoft GTSC in Bangalore, I was hired by Microsoft as a

full-time engineer on the Networking Team and I became a Technical Lead for the same team in 2005. I moved to Seattle in 2007 and since then I've been working solely on ISA. In 2008 I became a Technical Lead for the ISA Team and a few months later became a lead for the IAG Team as well. As a lead I mainly work on helping the engineers in my team with escalations. I also work with escalation engineers to collaborate with the ISA development team to resolve bugs and design change requests.

I generally spend my spare time with my wife, Anusha, and our little puppy, Mojo, who is a highly energetic springer spaniel. Much of my time is spent making sure that Mojo doesn't chew up the walls or my socks. However, he can make me smile anytime with his antics and he completes my family. I like to read a lot and whenever I can find some free time from work, wife, and the dog (not in that order), I generally try and read novels.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft
Press

Stay in touch!

To subscribe to the *Microsoft Press® Book Connection Newsletter*—for news on upcoming books, events, and special offers—please visit:

microsoft.com/learning/books/newsletter