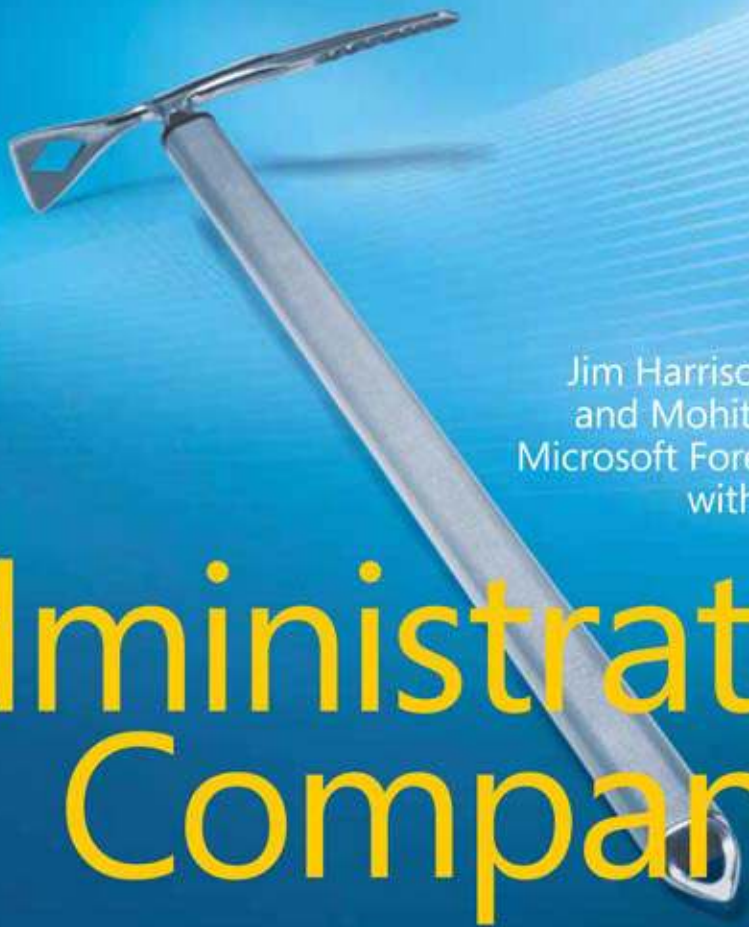
Microsoft

Foreword by David B. Cross
Product Unit Manager, Microsoft Forefront TMG 2010

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

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

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

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

PART IV TMG AS YOUR FIREWALL

Chapter 11 Configuring TMG Networks 209

Understanding Network Relationships 209
- Basic IP Routing 210
- Route Relationships 215
- NAT Relationships 215
- NAT Address Selection 218
- Network Rules 220

Creating Networks 222
- Built-In Networks 222
- Creating a New Network 224
- Creating a Network Rule 226

Configuring Your Protected Networks 231
- Authenticating Traffic from Protected Networks 233

Summary 240

Chapter 12 Understanding Access Rules 241

Traffic Policy Behavior 241
- Policy Engine Rule Basics 241
- Ping Access Rule Example 242
- CERN Proxy HTTP Example 245

Understanding Policy Re-Evaluation 249
- Policy Enforcement 250
- Exemptions in Policy Enforcement 252
- Policy Enforcement in Certain Scenarios 253

Troubleshooting Access Rules 253
- Basic Internet Access 254
- Authentication 256
- Name Resolution 259
- Using the Traffic Simulator 259

Summary 262

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

Configuring the Forefront TMG 2010 Cache 397
Enable Web Caching 397
Add a Cache Rule 400
Add a Content Download Job 407
CARP Configuration 413
Configuring the Intra-Array Address 415
Configuring the CARP Load Factor 416
Troubleshooting Cache 417
Analyzing Cache Behavior 417
Using CacheDir 420
Using FetchURL 421
Rebuilding the Cache 421
Summary. 424

PART VI TMG CLIENT PROTECTION

Chapter 17 Malware Inspection 427

Understanding Malware Inspection in TMG. 427
Configuring Malware Inspection 431
Configuring Malware Inspection for Your Environment 431
Defining Per-Rule Malware Inspection 442
Testing Internet Access with Malware Inspection 443
Creating Reports with Malware Statistics 446
Configuring a One-Time Report 447
Configuring a Recurring Report 451
Generating and Viewing Malware Inspection Reports 455
Customizing Malware Inspection Content in Reports 462
Summary. 463

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

Configuring the HTTP Filter 550
General Options 550
HTTP Methods 553
Extensions 555
Headers 557
Signatures 561
Summary. 570

PART VII TMG PUBLISHING SCENARIOS

Chapter 21 Understanding Publishing Concepts 573

Core Publishing Scenarios 573
Server Publishing 574
Server Publishing and Network Relationships 576
Server Publishing vs. Access Rules 577
Web Publishing 578
Publishing Rule Elements. 580
Elements in a Web Publishing Rule 580
Elements in a Server Publishing Rule 588
Planning Publishing Rules 591
Evaluating System Capacity 592
Protocol Considerations 593
Certificate Considerations 595
Load Balancing 595
Summary. 598

Chapter 22 Publishing Servers 599

How to Publish a Web Server 599
Publishing a Web Server Using HTTP Protocol 600
Publishing a Web Server Using HTTPS 618
Publishing a Non-Web Server. 637
Creating a Non-Web Server Publishing Rule 637

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

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