Marc Grote, Christian Gröbner, Dieter Rauscher

Das Handbuch

Insider-Wissen – praxisnah und kompetent

Microsoft® Forefront™ Threat Management Gateway 2010

Microsoft Press

Marc Grote, Christian Gröbner, Dieter Rauscher

Microsoft Forefront Threat Management Gateway 2010 Das Handbuch

Marc Grote, Christian Gröbner, Dieter Rauscher

Microsoft Forefront Threat Management Gateway 2010 Das Handbuch

Marc Grote, Christian Gröbner, Dieter Rauscher: Microsoft Forefront Threat Management Gateway 2010 – Das Handbuch
Microsoft Press Deutschland, Konrad-Zuse-Str. 1, D-85716 Unterschleißheim
Copyright © 2010 by Microsoft Press Deutschland

Das in diesem Buch enthaltene Programmmaterial ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor, Übersetzer und der Verlag übernehmen folglich keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programmmaterials oder Teilen davon entsteht.

Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen sowie E-Mail-Adressen und Logos sind frei erfunden, soweit nichts anderes angegeben ist. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen, E-Mail-Adressen und Logos ist rein zufällig.

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
10 09 08

ISBN 978-3-86645-127-8, PDF-eBook-ISBN 978-3-86645-387-6

© 2010 O'Reilly Verlag GmbH & Co. KG
Balthasarstr. 81, 50670 Köln
Alle Rechte vorbehalten

Fachlektorat: Georg Weiherer, Münzenberg
Korrektorat: Karin Baeyens, Judith Klein, Siegen
Layout und Satz: Cordula Winkler, mediaService, Siegen (www.media-service.tv)
Umschlaggestaltung: Hommer Design GmbH, Haar (www.HommerDesign.com)
Gesamtherstellung: Kösel, Krugzell (www.KoeselBuch.de)

Übersicht

Einleitung 21

Teil A
Grundlagen und Installation 29

1 Firewallgrundlagen 31

2 Windows Server 2008 R2 absichern 41

3 Einführung in die Forefront-Familie 53

4 Einführung in Forefront Threat Management Gateway 2010 71

5 Neuerungen in Forefront TMG 2010 77

6 Internetanbindung 87

Teil B
Allgemeine Konfiguration und Administration 109

7 Installieren von Forefront TMG 2010 111

8 Assistentengestützte Konfiguration 137

9 Konfigurieren von Forefront TMG 2010 145

10 Forefront TMG-Clients installieren und konfigurieren 261

11 Administration von Forefront TMG 2010 295

12 Spezielle Konfigurationen 317

13 Zertifikatverwaltung 333

Teil C
Betrieb von Forefront TMG 2010 371

14 Zugriffsregeln 373

15 Veröffentlichen von Exchange Server 447

16 Webveröffentlichungen 489

17 Serververöffentlichungen 575
18 E-Mail-Schutz 593
19 Eindringschutzsystem/Netzwerküberprüfungssystem 613
20 Voice over IP 635

Teil D
Virtuelle private Netzwerke 647
21 Virtuelle private Netzwerke 649
22 Clientanbindung mit VPN 659
23 VPN-Quarantänesteuerung 675
24 Standortverbindungen 691

Teil E
Forefront TMG 2010 Enterprise Edition 737
25 Microsoft Forefront TMG 2010 Enterprise Edition 739

Teil F
Überwachung und Fehlersuche 789
26 Überwachen von Forefront TMG 2010 791
27 Protokollierung und Berichte 835
28 Fehlersuche 851
29 Weiterführende Hilfe für Administratoren 877

Teil G
Anhang 887
A MCLS-Kurs und MCTS-Prüfung 889
B Die Autoren 895

Stichwortverzeichnis 899

Inhaltsverzeichnis

Einleitung 21
Das Buch 22
Die Zielgruppe des Buchs 22
Die Autoren 22
Die Beispielfirma Fabrikam Inc. 23
Der Inhalt im Überblick 25
Teil A – Grundlagen und Installation 25
Teil B – Allgemeine Konfiguration und Administration 26
Teil C – Betrieb von Forefront TMG 2010 26
Teil D – Virtuelle private Netzwerke 26
Teil E – Forefront TMG Enterprise Edition 26
Teil F – Überwachung und Fehlersuche 27
Anhang 27
Unser Dank 27
Wie können Sie Kontakt mit uns aufnehmen? 28

Teil A
Grundlagen und Installation 29

1 Firewallgrundlagen 31
Was ist eine Firewall? 32
Organisation 32
Software 32
Technik/Hardware 33
Firewallarten 33
Firewallkonfigurationen 36
Häufig verwendete Firewallkonfigurationen 36
Regelwerk 37
Umgebungssicherheit 37
Physische Sicherheit 38
Sicherheit der Peripherie 38
Kennwortrichtlinien 38
Risiko Mensch 38
Warum eine Firewall einsetzen? 39
Mythos Hardwarefirewall 39
Unterschiede zur Windows-Firewall 40
Zusammenfassung 40

2 Windows Server 2008 R2 absichern ... 41
Warum Windows Server absichern? ... 42
Wie sollten Sie Windows Server absichern? ... 42
Windows Update ... 42
Windows Server Update Services (WSUS) ... 44
Microsoft Baseline Security Analyzer ... 45
Gruppenrichtlinien ... 46
Sicherheitskonfiguration und -analyse ... 46
Dienste ... 47
Windows-Komponenten ... 48
TCP/IP-Filterung an der Netzwerkkarte ... 49
Umgebungssicherheit ... 49
Physische Sicherheit ... 50
Sicherheitsrichtlinie erstellen ... 50
Personal schulen und verantwortungsvoller Umgang mit den Firewallsystemen ... 50
Neuerungen in Service Pack 2 für Windows Server 2008 ... 51
Zusammenfassung ... 51

3 Einführung in die Forefront-Familie ... 53
Forefront-Produktportfolio im Kurzüberblick ... 54
Edge/Perimeter ... 54
Forefront Threat Management Gateway 2010 ... 54
Forefront Unified Access Gateway 2010 ... 55
Microsoft Forefront Threat Management Gateway Medium Business Edition ... 61
Serveranwendungen ... 62
Allgemeine Übersicht zu Forefront Server Security ... 62
Forefront Protection 2010 für Exchange ... 64
Forefront Protection 2010 für SharePoint ... 65
Forefront Security für Office Communication Server ... 65
Clientsicherheit ... 66
Forefront Client Security ... 66
Forefront Endpoint Protection 2010 ... 68
Verwaltung ... 68
Forefront Identity Manager 2010 ... 69
Forefront Server Security Management Console ... 69
Zusammenfassung ... 70

4 Einführung in Forefront Threat Management Gateway 2010 ... 71
Lizenzierung und Beschaffung ... 72
Appliance ... 73
Systemanforderungen ... 74
Zusammenfassung ... 75

5 Neuerungen in Forefront TMG 2010 ... 77

Neue Funktionen ... 78
- Verbesserte Erstkonfiguration ... 79
- Assistent für den Webzugriff ... 79
- Malwareschutz für den Webzugriff ... 79
- URL-Filterung ... 80
- HTTPS-Datenverkehr überprüfen ... 80
- Eindringschutzsystem ... 80
- E-Mails schützen ... 81
- Integrierte Updateverwaltung ... 81
- ISP-Redundanz ... 81
- Erweitertes NAT überstützen ... 82
- SSTP implementieren ... 82
- Neue Verschlüsselungsalgorithmen für IPsec-S2S-VPN-Verbindungen ... 82
- NAP zur VPN-Quarantänesteuerung integrieren ... 82
- SIP-Filter implementieren ... 83
- Konfiguration im Konfigurationsspeicherserver speichern ... 83

Fehlende Funktionen ... 84
- Ausgehende IP-Adresse pro Firewallrichtlinie ... 84
- Protokollbasiertes Routing ... 84
- Regelbasiertes Routing ... 85
- 1:1-NAT ... 85
- Unterstützung von SIP-TCP und SIP-TLS ... 85
- Bandbreitenregelung ... 86
- IPsec-Standort-zu-Standort-VPN-Verbindung mit dynamischen IP-Adressen ... 86

Zusammenfassung ... 86

6 Internetanbindung ... 87

Standleitung mit Router ... 88
DSL mit dynamischer IP-Adresse ... 92
DFÜ-Wählverbindung ... 95
Mehrere ISPs anbinden ... 98
- Failover ... 99
- Bündelung mit Lastverteilung ... 99
- Traffic-Shaping ... 100

Konzept der DNS-Auflösung ... 101
- DNS-Namensauflösung für interne Clients ... 101
- Split-DNS-Konfiguration ... 105

Zusammenfassung ... 107

Teil B
Allgemeine Konfiguration und Administration 109

7 Installieren von Forefront TMG 2010 111
Vorbereiten der Netzwerkumgebung 112
Netzwerkschnittstellen 112
Verbindungsreihenfolge 112
Protokollbindung 113
TCP/IP-Eigenschaften 114
Neuinstallation 118
Installation vorbereiten 119
Forefront TMG 2010 installieren 120
Update-Möglichkeiten 121
Einschränkungen der Update-Möglichkeiten 122
Forefront TMG 2010 auf einem Windows Server 2008 x64 installieren und Migration der Konfiguration von ISA Server 2006 122
Gründe für den Export einer Konfiguration 123
Aufgaben vor der Migration 124
Export und Import der Konfiguration 124
Evaluierungsversion 132
Virtualisierung 133
Zusammenfassung 136

8 Assistentengestützte Konfiguration 137
Assistentengestützte Konfiguration 138
Zusammenfassung 144

9 Konfigurieren von Forefront TMG 2010 145
Toolbox-Elemente konfigurieren 146
Protokolle 147
Benutzer 157
Inhaltstypen 159
Zeitpläne 160
Netzwerkobjekte 161
Netzwerkeinrichtung 172
Neues Netzwerkobjekt erstellen 173
Netzwerkbeziehung erstellen 176
Besondere Netzwerkkonfigurationen 178
Netzwerksätze 180
Netzwerkadapter 181
Systemrichtlinien 182
Grundlagen zu Firewallrichtlinien 193
Firewallrichtlinien verwalten 196

Cachekonfiguration ... 197
Webcache aktivieren ... 198
Cacheregeln konfigurieren ... 201
BITS-Caching ... 207
Geplanter Inhaltsdownload ... 209
HTTP-Komprimierung ... 214
Webverkettung ... 217
Webverkettung für bestimmte Ziele konfigurieren ... 217
Generelle Umleitung zu einem Upstreamserver ... 220
Anwendungs- und Webfilter ... 224
Anwendungsfilter ... 225
Webfilter ... 229
Routing ... 232
ISP-Redundanz ... 234
ISP-Redundanzmodus *Nur Failover* ... 235
ISP-Redundanzmodus *Lastenausgleich mit Failoverfunktion* ... 235
Voraussetzungen für die ISP-Redundanz ... 235
Verfügbarkeitsüberprüfung der ISP-Redundanz ... 236
ISP-Redundanz konfigurieren ... 237
ISP-Redundanz verwalten und überwachen ... 243
DiffServ-Filter ... 245
DiffServ ... 246
Update Center ... 249
Fehlersuche zur Signaturaktualisierung ... 255
Kundenfeedback ... 257
Telemetrie ... 259
Zusammenfassung ... 259

10 Forefront TMG-Clients installieren und konfigurieren ... 261
Der SecureNAT-Client ... 262
Der Webproxyclient ... 264
Proxyeinstellungen manuell konfigurieren ... 266
Proxyeinstellungen über Gruppenrichtlinien konfigurieren ... 268
Proxyeinstellungen automatisch suchen ... 271
Der Forefront TMG-Client ... 278
Funktionsweise des Forefront TMG-Client ... 279
Forefront TMG-Clients bereitstellen ... 280
Forefront TMG-Client konfigurieren ... 280
Forefront TMG-Clientinstallation ... 281
Manuelle Installation ... 282
Forefront TMG-Clienteinstellungen definieren ... 284
Zusammenfassung ... 294

11 Administration von Forefront TMG 2010 ... **295**
Verwaltung per Remotedesktop ... **296**
Verwaltung mit der Forefront TMG 2010-Verwaltungskonsole ... **299**
Administrative Rollen zuweisen ... **301**
Konfiguration exportieren und sichern ... **303**
Gesamtkonfiguration exportieren ... **304**
Teile der Konfiguration exportieren ... **306**
Konfiguration per Skript exportieren ... **308**
Konfiguration importieren und wiederherstellen ... **310**
Konfiguration wiederherstellen ... **310**
Konfigurationsteile importieren und wiederherstellen ... **312**
Microsoft Forefront TMG Best Practices Analyzer Tool ... **314**
Microsoft Forefront TMG Best Practices Analyzer Tool installieren ... **314**
Konfiguration durch Microsoft Forefront TMG Best Practices Analyzer überprüfen ... **315**
Zusammenfassung ... **316**

12 Spezielle Konfigurationen ... **317**
Forefront TMG 2010 mit einer Netzwerkkarte ... **319**
Forefront TMG 2010 mit einer DMZ ... **321**
Umkreisnetzwerk mit öffentlichen IP-Adressen ... **322**
Umkreisnetzwerk mit privaten IP-Adressen ... **323**
IP-Konfiguration von Forefront TMG 2010 mit einer DMZ ... **324**
Forefront TMG 2010 mit mehreren Netzwerkkarten ... **325**
Forefront TMG 2010 im Front-End/Back-End-Szenario ... **328**
Back-End-Firewall mit Routebeziehung ... **329**
Back-End-Firewall mit NAT-Beziehung ... **330**
Forefront TMG 2010 auf einem Domänencontroller ... **331**
Zusammenfassung ... **332**

13 Zertifikatverwaltung ... **333**
Grundlagen ... **334**
Das Zertifikat ... **335**
Die Zertifizierungsstelle ... **336**
Public Key-Infrastruktur (PKI) ... **338**
Dateiformate von Zertifikaten ... **339**
Zertifizierungsstelle installieren ... **340**
Zertifikatbeantragung ... **344**
Zertifikat über das Snap-In *Zertifikate* beantragen ... **344**
Zertifikat über die Registrierungswebsite beantragen ... **349**
Zertifikate am Server mit Forefront TMG 2010 beantragen ... **352**
Zertifikatexport und -import ... **354**
Zertifikate exportieren ... **354**
Zertifikate importieren ... **356**

Zertifikate in Webveröffentlichungen verwenden ... 357
Grundlagen der SSL-Verschlüsselung ... 357
Zertifikate in Forefront TMG 2010 verwenden ... 358
SAN-Zertifikate ... 359
Interne Zertifizierungsstelle für SAN-Zertifikate konfigurieren ... 360
SAN-Zertifikat beantragen ... 360
Zertifikatsperrliste veröffentlichen ... 362
Sperrlisten-Verteilungspunkt hinzufügen ... 363
Zertifikatsperrliste über Forefront TMG 2010 veröffentlichen ... 364
Webveröffentlichung durch die HTTP-Filterung absichern ... 366
Zertifikatsperrung in Forefront TMG 2010 konfigurieren ... 367
SelfSSL verwenden ... 368
Zusammenfassung ... 370

Teil C
Betrieb von Forefront TMG 2010 ... 371

14 Zugriffsregeln ... 373
Systemrichtlinien ... 374
Zugriff auf DNS-Server einschränken ... 374
Zugriff auf Active Directory einschränken ... 375
Zugriff auf Webserver erlauben ... 376
Nicht benötigte Systemrichtlinien deaktivieren ... 377
Eingeschränkter Zugriff für Server ... 378
Zugriff auf DNS-Server ... 379
Zugriff auf externe Zeitserver ... 381
Server für den Zeitabgleich konfigurieren ... 384
Zugriff auf Windows Update ... 385
Zugriff auf Forefront Signaturupdates ... 389
Eingeschränkter Zugriff für Clients ... 392
Zugriffsregeln für den Webzugriff planen ... 393
Zugriffsregel für den Webzugriff erstellen ... 393
Zugriff auf bestimmte Websites sperren ... 395
HTTP-Filterung ... 398
Zugriffsregel für den FTP-Zugriff erstellen ... 405
Zugriffsregel für den Zugriff auf einen externen Mailserver erstellen ... 408
Webzugriffsrichtlinie ... 410
Webzugriffsrichtlinie mit dem Assistenten konfigurieren ... 411
URL-Filterung ... 416
Malwareüberprüfung ... 428
HTTP ohne Webproxyfilter ... 436
HTTPS-Überprüfung ... 437
Zusammenfassung ... 445

15 Veröffentlichen von Exchange Server ... **447**
Grundlagen von SMTP ... **448**
SMTP-Serververöffentlichung ... **452**
Outlook Web App veröffentlichen ... **457**
Vorbereitende Konfiguration von Exchange Server 2010 ... **457**
Webveröffentlichungsregel für Outlook Web App erstellen ... **458**
Absicherung mithilfe der HTTP-Filterung ... **463**
Outlook Anywhere veröffentlichen ... **467**
Vorbereitende Konfiguration von Exchange Server 2010 ... **468**
Veröffentlichungsregel für Outlook Anywhere in Forefront TMG 2010 erstellen ... **469**
Absicherung durch die HTTP-Filterung ... **473**
Outlook 2010 konfigurieren ... **475**
Exchange-ActiveSync veröffentlichen ... **477**
Exchange Server 2010 vorbereiten ... **478**
Veröffentlichungsregel für Exchange-ActiveSync erstellen ... **479**
Absicherung durch die HTTP-Filterung ... **480**
ActiveSync auf dem Endgerät konfigurieren ... **482**
Fehlerbehebung ... **483**
BlackBerry ... **486**
Zusammenfassung ... **488**

16 Webveröffentlichungen ... **489**
Webveröffentlichung ... **490**
HTTP-Website veröffentlichen ... **490**
Durch HTTPS gesicherte Website veröffentlichen ... **508**
SharePoint-Site veröffentlichen ... **522**
Linkübersetzung ... **526**
Remotedesktopdienste veröffentlichen ... **528**
Remotedesktopgateway veröffentlichen ... **529**
Web Access für Remotedesktop veröffentlichen ... **536**
Authentifizierungsmethoden ... **540**
Standardauthentifizierung ... **540**
Digest- und WDigest-Authentifizierung ... **541**
Integrierte Windows-Authentifizierung (NTLM und Kerberos) ... **541**
RSA SecurID ... **541**
Formularbasierte Authentifizierung ... **542**
Single Sign-On ... **542**
Zertifikatbasierte Authentifizierung ... **542**
RADIUS (Remote Access Dial-In User Service) ... **543**
RADIUS-Einmalkennwörter ... **543**
LDAP (Lightweight Directory Authentication Protocol) ... **543**
Konfiguration der Authentifizierungsmethoden ... **543**
LDAP konfigurieren ... **544**
LDAP-Serversatz erstellen ... **544**

RADIUS ... 548
Grundlagen ... 548
Sicherheitsaspekte beim Einsatz von RADIUS ... 549
Serverrolle *Netzwerkrichtlinien- und Zugriffsdienste* installieren ... 549
RADIUS-Server in Active Directory registrieren ... 550
Forefront TMG 2010 als RADIUS-Client im Netzwerkrichtlinienserver hinzufügen ... 550
RADIUS-Unterstützung in Forefront TMG 2010 ... 551
Nachteile der RADIUS-Authentifizierung mit Forefront TMG 2010 ... 551
Zugriffsregel zur Verwendung von RADIUS erstellen ... 553
RADIUS-Server veröffentlichen ... 554
Netzwerkrichtlinienserver (NPS) ... 554
Netzwerkzugriffsschutz (NAP) ... 557
Webserver-Lastenausgleich ... 558
Lastenausgleichsmodi ... 558
Webfarm-Einstellungen ... 571
Zusammenfassung ... 573

17 Serververöffentlichungen ... 575
Grundlagen ... 576
Internen Remotedesktopdienste-Server veröffentlichen ... 577
Grundlagen zum Remotedesktopprotokoll ... 577
Serververöffentlichung unter Verwendung der Standardeinstellungen erstellen ... 578
Serververöffentlichung mit Abweichungen von den Standardeinstellungen erstellen (Portadressübersetzung) ... 583
Forefront TMG 2010 als DHCP-Server ... 587
DHCP-Serverrolle einrichten ... 587
Neue Zugriffsregel erstellen ... 588
Zusammenfassung ... 591

18 E-Mail-Schutz ... 593
Installationsreihenfolge der Komponenten für den E-Mail-Schutz ... 594
Exchange Server 2010 Edge Transport Server ... 594
Sprachoptionen auswählen ... 595
Edge-Transport-Rolle installieren ... 596
Systemvoraussetzungen prüfen ... 596
Forefront Protection 2010 für Exchange Server installieren ... 598
E-Mail-Richtlinie konfigurieren ... 600
Forefront TMG 2010-Systemrichtlinien aktivieren ... 603
EdgeSync konfigurieren ... 604
Antispam- und Antiviruskonfiguration ... 605
Microsoft Exchange Server lizenzieren ... 608
Erweiterte Eigenschaften konfigurieren ... 608
Forefront Protection 2010 für Exchange Server lizenzieren ... 609
Erweiterte Forefront Protection für Exchange-Konfiguration ... 610
Zusammenfassung ... 611

19 Eindringschutzsystem/Netzwerküberprüfungssystem ... **613**
Netzwerküberprüfungssystem (NIS) ... **614**
Zero-Day-Vulnerability ... **615**
Generic Application-Level Protocol Analyzer ... **615**
NIS in Forefront TMG 2010 konfigurieren ... **616**
Verhaltensbasierte Eindringversuchserkennung ... **623**
Wurmausbreitung ... **623**
TCP-Massenangriffe ... **624**
SYN-Angriffe ... **624**
HTTP-Denial-of-Service-Angriffe ... **624**
Nicht-TCP-DDoS-Angriffe (verteilte Denial-of-Service-Angriffe) ... **624**
UDP-Massenangriffe ... **624**
Eindringschutz für allgemeine Angriffe ... **624**
Flutabwehreinstellungen konfigurieren ... **630**
Alarmdefinitionen für IDS und IPS ... **633**
Zusammenfassung ... **634**

20 Voice over IP ... **635**
Grundlagen zu VoIP ... **636**
Forefront TMG 2010 für VoIP-Verbindungen konfigurieren ... **637**
Forefront TMG 2010 für ausgehende VoIP-Verbindungen ohne IP-Telefonanlage konfigurieren ... **637**
Forefront TMG 2010 für VoIP-Verbindungen mit einer internen IP-Telefonanlage konfigurieren ... **639**
Einschränkungen in Forefront TMG 2010 zur Nutzung von VoIP ... **645**
Zusammenfassung ... **646**

Teil D
Virtuelle private Netzwerke ... **647**

21 Virtuelle private Netzwerke ... **649**
Grundlagen zu VPN-Netzwerken ... **650**
PPTP ... **651**
L2TP/IPsec ... **652**
IPsec ... **653**
SSTP ... **656**
Zusammenfassung ... **657**

22 Clientanbindung mit VPN ... **659**
Konfigurieren von Forefront TMG 2010 für eingehende VPN-Clientverbindungen ... **660**
Konfigurieren von Forefront TMG 2010 ... **660**
Konfigurieren der VPN-Clientverbindungen ... **666**
Konfiguration des Clients für VPN-Clientverbindungen ... **666**
Verbindungskonfiguration für das PPTP-Protokoll ... **668**
Verbindungskonfiguration für das L2TP/IPsec-Protokoll ... **669**

Verbindungskonfiguration für das SSTP-Protokoll ... 671
Konfiguration von Split-Tunneling ... 671
Konfiguration der Proxyeinstellungen für VPN-Clients ... 672
Zusammenfassung ... 673

23 VPN-Quarantänesteuerung ... 675
Grundlagen zur VPN-Quarantänesteuerung ... 676
Möglichkeiten der VPN-Quarantänesteuerung ... 676
VPN-Quarantänesteuerung in Forefront TMG 2010 konfigurieren ... 677
VPN-Quarantänesteuerung aktivieren ... 677
Authentifizierungseinstellungen konfigurieren ... 678
Netzwerkrichtlinienserver konfigurieren ... 679
Neuen RADIUS-Client einrichten ... 679
Systemintegritätsprüfung konfigurieren ... 680
Systemintegritätsrichtlinien erstellen ... 681
Netzwerkrichtlinien erstellen ... 682
Verbindungsanforderungsrichtlinie konfigurieren ... 684
Client für NAP konfigurieren ... 685
NAP-Dienst aktivieren und starten ... 686
Remotezugriffs-Quarantäneerzwingungsclient aktivieren ... 686
VPN-Verbindung für NAP konfigurieren ... 687
VPN-Clients überwachen ... 689
Zusammenfassung ... 690

24 Standortverbindungen ... 691
Istzustand der Firma Fabrikam Inc. ... 692
Grundlagen zu Standortverbindungen ... 693
Standort-zu-Standort-VPN-Verbindung mit PPTP einrichten ... 694
Forefront TMG 2010 am Standort München konfigurieren ... 694
Forefront TMG 2010 am Standort Hamburg konfigurieren ... 701
Standort-zu-Standort-VPN-Verbindung mit L2TP/IPsec einrichten ... 703
Forefront TMG 2010 am Standort München konfigurieren ... 703
Forefront TMG 2010 am Standort Zürich konfigurieren ... 709
Standort-zu-Standort-VPN-Verbindung mit IPsec einrichten ... 713
Standort-zu-Standort-VPN-Verbindung mit dem IPsec-Protokoll in Forefront TMG 2010 konfigurieren ... 714
Cisco ASA 5505 konfigurieren ... 721
LANCOM 1724 VoIP konfigurieren ... 725
Sonicwall TZ 180 konfigurieren ... 730
Zusammenfassung ... 735

Teil E
Forefront TMG 2010 Enterprise Edition 737

25 Microsoft Forefront TMG 2010 Enterprise Edition 739
Neuerungen in Forefront TMG 2010 Enterprise Edition 740
Merkmale von Forefront TMG 2010 Enterprise Edition 740
Vergleich von Forefront TMG 2010 Standard mit Forefront TMG 2010 Enterprise Edition 743
Forefront TMG 2010 Enterprise Edition installieren und konfigurieren 744
Forefront TMG 2010 Enterprise auf einem Domänencontroller 745
Systemanforderungen 745
Forefront TMG 2010 Enterprise auf TMG-MUC1 und TMG-MUC2 installieren 745
Enterprise Management Server 746
Forefront TMG 2010-Array umbenennen 746
Kommunikation 746
Hostkennung 747
Verbindung mit einem Enterprise Management Server herstellen 747
Unternehmensnetzwerke 748
Berechtigungsdelegation und Forefront TMG 2010-Rollen 749
Zentrale Protokollierung 751
VPN-Besonderheiten 751
Firewallrichtlinien auf Unternehmens- und Arrayebene 751
Von ISA Server 2006 Enterprise Edition auf Forefront TMG 2010 Enterprise migrieren 754
Updateprozess 754
Forefront TMG 2010 Enterprise Management Server installieren und konfigurieren 756
Cache Array Routing Protocol konfigurieren 772
Cache Array Routing Protocol einrichten 773
Netzwerklastenausgleich konfigurieren 774
NLB an Forefront TMG 2010 einrichten 776
Windows-Netzwerkkonfiguration für NLB 779
ADAM Sites Tool 785
Zusammenfassung 788

Teil F
Überwachung und Fehlersuche 789

26 Überwachen von Forefront TMG 2010 791
Übersicht 792
Alarme 793
Sitzungen 819
Konnektivitätsverifizierungen 820
Dienste 825
Konfiguration 827
Änderungsnachverfolgung 827

Produktversion herausfinden ... 830
Drittthersteller-Tools ... 831
Bandwidth Splitter für Microsoft Forefront TMG 2010 ... 832
TrafficQuota ... 832
CyBlock für ISA Server und Forefront TMG 2010 ... 832
GFI WebMonitor 2009 für ISA Server und Forefront TMG 2010 ... 833
Burstek WebFilter ... 833
Zusammenfassung ... 834

27 Protokollierung und Berichte ... 835
Protokollierungsmöglichkeiten ... 836
Protokollierung konfigurieren ... 836
Protokollwarteschlange konfigurieren ... 841
Ausnahme von Datenverkehr aus der Protokollierung ... 842
Berichterstellung ... 843
Einmalige Berichte erstellen ... 843
Erstellen von wiederkehrenden Berichten ... 846
Einstellungen zur Berichterstattung festlegen ... 848
Zusammenfassung ... 849

28 Fehlersuche ... 851
Protokolle auswerten ... 852
Protokolltextfarben anpassen ... 854
Datenverkehr von einem bestimmten Client herausfiltern ... 854
Datenverkehr mit einem bestimmten Protokoll herausfiltern ... 855
Bereits gesendeten Datenverkehr herausfiltern ... 856
Netzwerktools ... 857
Zusatztools ... 861
ADAM Sites-Tool ... 861
Forefront TMG 2010 Software Development Kit ... 862
Microsoft Netzwerkmonitor ... 870
Neuerungen des Netzwerkmonitor 3.3 ... 870
Aktives und passives FTP ... 873
Filterung von Netzwerkverkehr ... 874
Besonderheiten zum Microsoft Netzwerkmonitor ... 875
Zusammenfassung ... 876

29 Weiterführende Hilfe für Administratoren ... 877
Veranstaltungen ... 878
Microsoft TechNet-Veranstaltungen ... 878
Microsoft TechEd ... 879
User Groups ... 879
Exchange User Group ... 879
Forefront User Group ... 879
Microsoft Partner-Stammtisch ... 880

Online-Communities ... 880
Newsgroups ... 880
Webforen ... 882
Websites ... 883
www.microsoft.com/germany/forefront/ ... 883
www.msisafaq.de ... 883
www.isaserver.org ... 883
Blogs ... 884
Dieter Rauschers Forefront Blog ... 884
Forefront TMG Blog ... 884
Microsoft Forefront Server Security Blog ... 885
Microsoft Forefront TMG-Team ... 885
Microsoft TechNet ... 885
Microsoft Knowledge Base ... 885
Zusammenfassung ... 886

Teil G
Anhang ... 887

A MCLS-Kurs und MCTS-Prüfung ... 889
MCLS/MOC-Kurs ... 890
Kursinhalt ... 890
MCTS-Prüfung ... 894

B Die Autoren ... 895
Marc Grote ... 896
Christian Gröbner ... 896
Dieter Rauscher ... 897

Stichwortverzeichnis ... 899

Einleitung

Das Buch	22
Die Zielgruppe des Buchs	22
Die Autoren	22
Die Beispielfirma Fabrikam Inc.	23
Der Inhalt im Überblick	25
Unser Dank	27
Wie können Sie Kontakt mit uns aufnehmen?	28

Das Buch

Ob Sie dieses Buch gekauft, geschenkt bekommen oder ausgeliehen haben – vielen Dank, dass Sie sich dafür entschieden haben. Sicherlich haben Sie das nicht getan, um uns Autoren eine Freude zu bereiten, sondern interessieren sich für dieses Thema, weil Sie vielleicht eine Version von *Internet Security and Acceleration Server* einsetzen und erfahren wollen, was es Neues gibt. Eventuell sind Sie aber auch ein Neueinsteiger? Wir sind uns darüber klar, dass Sie keinen Roman oder Krimi erwarten. Daher haben wir uns Mühe gegeben, so viel technische Informationen zu liefern wie möglich. Das bedingt manchmal, dass der eine oder andere Abschnitt eher trocken ist.

Mit Forefront Threat Management Gateway 2010 bringt Microsoft nach gut dreieinhalb Jahren die Nachfolgeversion von *Internet Security and Acceleration Server 2006* heraus, die konsequent weiterentwickelt wurde. Aber dazu werden Sie in diesem Buch noch einiges lesen.

Die Zielgruppe des Buchs

Dieses Buch richtet sich hauptsächlich an Administratoren, die bei sich Forefront TMG 2010 einsetzen oder den Einsatz planen. IT-Berater werden hier ebenfalls viele nützliche Details finden, um ihre Projekte erfolgreich umsetzen zu können.

Sie werden den Inhalt dieses Buchs besser verstehen und nutzen können, wenn Sie zumindest über grundlegende Kenntnisse zu Windows Server 2008, Netzwerkprotokollen und Firewallfunktionen verfügen.

Die Autoren

Das Autorenteam dieses Buchs hat für Microsoft Press bereits die Handbücher zu *Internet Security and Acceleration Server 2004* und *Internet Security and Acceleration Server 2006* geschrieben. Darüber hinaus haben wir auch einzeln an verschiedenen weiteren Buchprojekten gearbeitet. Eine Auflistung dazu finden Sie im Anhang. Gemeinsam kennzeichnet uns die Leidenschaft für Community-Arbeit und Forefront, wofür wir seit Jahren von Microsoft mit dem MVP-Award ausgezeichnet wurden.

HINWEIS Der Titel »Microsoft Most Valuable Professional« [MVP] wird von Microsoft jährlich an ausgewählte Spezialisten vergeben, die sich durch außerordentlichen Einsatz, hohe fachliche Kompetenz und ein herausragendes Kommunikationstalent in Communities rund um Microsoft-Produkte und -Technologien einen Namen gemacht haben. Mehr Informationen zum MVP-Programm finden Sie auf der Website *http://www.microsoft.com/mvp*.

Marc Grote ist seit 21 Jahren im IT-Bereich als Administrator, Consultant und Trainer in Nienstaedt mit den Schwerpunkten Forefront TMG, FCS, FSE, Microsoft Windows Server und Exchange Server tätig. Er besitzt umfangreiche Erfahrung mit den Produkten Microsoft Proxy Server 2.0 bis Microsoft Forefront TMG 2010, aber auch mit Firewallprodukten von Drittherstellern. Seit Juli 2004 ist Marc Grote MVP. Damit wurde er für sein Engagement in den Microsoft ISA Server-, Exchange- und Windows Server-Newsgroups ausgezeichnet.

Christian Gröbner ist seit 11 Jahren als Administrator und Consultant für Planung und Realisierung von Netzwerken tätig. Seine Erfahrungen liegen im Bereich Microsoft ISA Server/Forefront, Microsoft Exchange, Windows Server mit dem Schwerpunkt Netzwerksicherheit. Für sein Engagement in der Microsoft Newsgroup wurde Christian Gröbner seit Januar 2004 der Titel »Microsoft Most Valuable Professional« verliehen.

Dieter Rauscher ist als IT-Manager und Berater in München tätig. Seine Schwerpunkte liegen in der Planung und Verwaltung von Infrastrukturen mit Forefront TMG, ISA Server, Exchange Server und Windows Server. Neben zahlreichen Veröffentlichungen rund um ISA Server und Forefront ist er sehr aktiv in den Microsoft Newsgroups und Foren zu Forefront und Exchange Server. Gemeinsam mit Christian leitet er die Forefront User Group. In München organisiert und leitet er die regelmäßigen Microsoft Partner Technical Community-Treffen. Darüber hinaus trifft man ihn regelmäßig auf Veranstaltungen und Konferenzen zu Messaging und Security an. Seit Oktober 2002 wurde er jedes Jahr erneut mit dem Titel »Microsoft Most Valuable Professional« ausgezeichnet.

Die Beispielfirma Fabrikam Inc.

Mit unserem ersten Buch, dem ISA Server 2004-Handbuch, haben wir mit dem Versuch begonnen, IT-Fachbücher praxisnäher zu schreiben. Wir haben damals die fiktive Firma *Fabrikam Inc.* eingeführt, Benutzern Namen gegeben, für Beispiele »echte« IP-Adressen und Domänennamen verwendet sowie versucht, so gut wie möglich bestimmte Szenarien anhand alltäglicher Anforderungen und Anwenderverhalten zu beschreiben. Leider ist das jedoch nicht für jedes Kapitel so umsetzbar.

HINWEIS Falls Sie sich jetzt fragen, warum wir ausgerechnet den Namen *Fabrikam Inc.* ausgesucht haben – hier die Antwort:

Aus namensrechtlichen Gründen können und dürfen wir keine real existierenden Namen verwenden, an denen wir nicht auch die Rechte haben. Microsoft jedoch hat für solche Zwecke mehrere Namensgebrauchsrechte, die wir hier einsetzen können. Wenn Sie viel im Microsoft-Umfeld tätig sind, haben Sie sicher auch schon von *Contoso* oder *Woodgroove Bank* gehört. Fabrikam Inc. ist quasi eine Schwester dazu. Ähnlich ist es mit den in diesem Buch verwendeten öffentlichen IP-Adressen. Diese sind auf Microsoft registriert und werden von uns zur besseren Veranschaulichung der Beispiele verwendet.

Bestätigt durch die Rückmeldungen zu den vergangenen drei Büchern werden wir auch in diesem vorliegenden Buch an diesem Konzept festhalten.

Fabrikam Inc. hat sich natürlich in den vergangenen Jahren (ISA Server 2006 wurde ja vor gut drei Jahren bei Fabrikam Inc. eingeführt) weiterentwickelt und vergrößert. Die IT-Infrastruktur und die Anforderungen daran sind gewachsen, was uns in diesem Buch zugute kommt. Neue Standorte sind bereits oder werden noch hinzukommen, mehr Mitarbeiter erfordern eine bessere Stabilität und auch höhere Anforderungen an die Verfügbarkeit. Lassen Sie sich überraschen!

Im vergangenen Jahr wurden bei Fabrikam Inc. die meisten Server auf Windows Server 2008 R2 aktualisiert und die Einführung von Windows 7 ist fast abgeschlossen. Ebenso ist der Übergang zu Exchange Server 2010 nahezu beendet. Die bestehenden Volumenlizenzverträge wurden verlängert und erweitert. Michael Berger versucht, so gut wie möglich auf dem aktuellen Stand der Technik zu bleiben und testet neue Produktversionen so früh wie möglich aus – was dank der Virtualisierungstechnik wesentlich einfacher ist wie vor einigen Jahren.

Die einzelnen für dieses Buch relevanten Server werden Sie im weiteren Verlauf näher kennen lernen. Von nun an werden Sie als Leser in die Rolle von Michael Berger versetzt und alle hier beschriebenen Konfigurationen aus seiner Sicht durchführen. Wir hoffen, Ihnen hiermit den Einsatz und Umgang mit Forefront Threat Management Gateway 2010 zu erleichtern.

Um Ihnen Fabrikam Inc. näher zu bringen, finden Sie nachfolgend eine Übersicht:

Die *Fabrikam I nc.* ist ein Beratungsunternehmen mit Hauptsitz in München und vier weiteren Standorten in Hamburg, Zürich, Prag und London. Die meisten Mitarbeiter sind viel auf Reisen und benutzen daher fast ausschließlich Notebooks. Das Unternehmen verfügt über folgende wesentliche Infrastrukturkomponenten, die in Tabelle E.1 aufgeführt werden.

Tabelle E.1 Übersicht der Server und Arbeitsstationen

ISA-MUC	ISA Server 2006 am Standort München
ISA-HH	ISA Server 2006 am Standort Hamburg
TMG-MUC	TMG 2010 am Standort München
TMG-LON	TMG 2010 am Standort London
DC-MUC	Windows Server 2008 R2 Domänencontroller am Standort München
DC-HH	Windows Server 2008 R2 Domänencontroller am Standort Hamburg
DC-ZRH	Windows Server 2008 R2 Domänencontroller am Standort Zürich
DC-LON	Windows Server 2008 R2 Domänencontroller am Standort London
HV-MUC	Windows Server 2008 R2 mit der Hyper-V-Rolle
MSX-MUC	Exchange Server 2010 als Groupwareserver
PC-0x	Workstations mit Windows 7
NB-0x	Notebooks mit Windows 7

Die Tabelle E.2 führt die Mitarbeiter auf, die für die Beispiele im Buch wichtig sind:

Tabelle E.2 Mitarbeiterübersicht von Fabrikam Inc.

Franz Maier	Geschäftsführer
Michael Berger	IT-Administrator
Tobias K lein	Berater mit Außendiensttätigkeit
Marietta Roth	Beraterin mit Außendiensttätigkeit
Sylke Burghart	Buchhalterin

Der Standort München ist derzeit durch einen ISA Server 2006 mit einer 100 Mbit/s-Standleitung und öffentlichen IP-Adressen an das Internet angebunden. Der ISA Server soll dringend durch Forefront TMG 2010 auf einer neuen Hardware abgelöst werden. Dabei ist es wichtig, die bestehende Konfiguration so weit wie möglich zu übernehmen. Am Standort London ist ein DSL-Anschluss vorhanden, der durch einen neuen Forefront TMG 2010 an das Firmennetzwerk angebunden werden soll.

Alle Standorte von Fabrikam Inc. sind durch Direktverbindungen eines europäischen Internet Service Providers angebunden und teilen sich den Internetzugang in München, verfügen dadurch aber auch über die Möglichkeit, eine der IP-Adressen zu nutzen und eine direkte Internetanbindung zu ermöglichen.

Folgende IP-Konfigurationen werden bei Fabrikam Inc. in diesem Buch verwendet:

- **München**
  - IP-Subnetz: 172.19.11.0/24
  - TMG-MUC: 172.19.11.1 (gleichzeitig Standardgateway)
  - DC-MUC: 172.19.11.2 (gleichzeitig DC, GC, DNS-Server)
- **Hamburg**
  - IP-Subnetz: 10.10.10.0/24
  - TMG-HH: 10.10.10.1 (gleichzeitig Standardgateway)
  - DC-HH: 10.10.10.2 (gleichzeitig DC, GC, DNS-Server)
- **Zürich**
  - IP-Subnetz: 10.20.20.0/24
  - TMG-ZRH: 10.20.20.1 (gleichzeitig Standardgateway und DHCP-Server)
  - DC-ZRH: 10.20.20.2 (gleichzeitig DC, GC, DNS-Server)
- **London**
  - IP-Subnetz: 10.30.30.0/24
  - TMG-LON: 10.30.30.1 (gleichzeitig Standardgateway)
  - DC-LON: 10.30.30.2 (gleichzeitig DC, GC, DNS-Server)
- **Öffentliches Netzwerk**
  - IP-Subnetz: 207.46.130.104/29

Der Inhalt im Überblick

Dieses Buch ist in mehrere Teile gegliedert, die in etwa den Phasen der Planung, Implementierung und Wartung von Forefront TMG 2010 entsprechen. Auf den folgenden Seiten geben wir Ihnen einen schnellen Überblick, was Sie alles erwartet.

Teil A – Grundlagen und Installation

Dieser Teil beschäftigt sich zuerst mit den grundlegenden Informationen rund um das Thema Firewall im Allgemeinen. Sie lernen den Begriff »Firewall« richtig zu verstehen und einzusetzen. Nach einem kleinen Ausflug in die sichere Konfiguration von Windows Server 2008 R2 stellen wir Ihnen die Forefront Familie richtig vor. Nein, das ist keine virtuelle Familie aus der Firma Fabrikam Inc., sondern es handelt sich um eine Produktfamilie von Microsoft. Doch lesen Sie selbst! Nach der Familienvorstellung beginnt endlich die Einführung in Forefront TMG 2010. Nach einem Vergleich der Funktionen mit der Vorgängerversion Internet Security and Acceleration Server 2006 geht es

direkt zur Installation. Hier lernen Sie, welche Internetanbindungen Forefront TMG 2010 unterstützt und was dazu berücksichtigt werden muss. Danach sehen Sie, wie Forefront TMG 2010 installiert wird und welche Möglichkeiten es gibt, von einer Vorgängerversion umzusteigen.

Teil B – Allgemeine Konfiguration und Administration

Dieser Teil baut auf die in Teil A erfolgte Installation auf und bringt Ihnen die ersten Schritte in der Konfiguration bei. Wir erklären Ihnen sämtliche Funktionen. Sie lernen dabei, wie Sie Forefront TMG 2010 optimal für den anschließenden Betrieb einrichten können. Dieser Teil ist besonders wichtig, da alle weiteren Kapitel in diesem Buch darauf aufsetzen. Sie finden in diesem Teil Informationen über die notwendige Clientkonfiguration, den Zugang zur Forefront TMG 2010-Verwaltung, Sicherung und Wiederherstellung und den Umgang mit Zertifikaten. Ergänzend zeigen wir Ihnen, in welchen Umgebungen Forefront TMG 2010 eingesetzt werden kann.

Teil C – Betrieb von Forefront TMG 2010

Nachdem Sie im vorangegangenen Teil gelernt haben, Forefront TMG 2010 erfolgreich zu installieren und grundsätzlich einzurichten, geht es in diesem Teil um den täglichen Betrieb. Wir zeigen Ihnen in diesem Kapitel, wie Sie das Regelwerk von Forefront TMG 2010 nutzen können, um den internen Clientcomputern einen sicheren Webzugriff zu ermöglichen und wie Sie interne Ressourcen wie Webserver oder Terminalserver für externe Benutzer zugänglich machen können. Darüber hinaus erfahren Sie, wie der E-Mail-Verkehr Ihres Unternehmens wirkungsvoll abgesichert werden kann und Sie gleichzeitig bestmöglich von Spam und Viren verschont werden.

Teil D – Virtuelle private Netzwerke

In diesem Teil geht es um die Anbindung von mobilen Computern, Heimarbeitsplätzen oder ganzen Zweigstellen an Ihr Unternehmensnetzwerk. Im Gegensatz zu den in den bisherigen Kapiteln erklärten Möglichkeiten, gezielt einzelne Dienste und Anwendungen zu veröffentlichen, können VPN-Verbindungen genutzt werden, um ein Arbeiten wie direkt im Büro zu ermöglichen.

Da es gerade bei Standortanbindungen viele unterschiedliche Geräte an den Gegenstellen geben kann, zeigen wir auch anhand einiger ausgewählter Produkte, wie das auch ohne ein Forefront TMG 2010 auf der anderen Seite geht.

Teil E – Forefront TMG Enterprise Edition

Dieser Teil beschreibt – weitgehend losgelöst vom restlichen Buch – detailliert die Besonderheiten und Zusatzfunktionen der Enterprise Edition von Forefront TMG 2010.

Teil F – Überwachung und Fehlersuche

Diesen letzten großen Teil dieses Buchs können wir Ihnen leider nicht ersparen. Sie werden sich an dieses Kapitel sicher noch erinnern, auch wenn Sie dieses Buch schon längst beiseitegelegt haben. Es geht überwiegend darum, was zu tun ist, wenn mal was nicht so läuft wie es sein sollte. Wie kann Forefront TMG 2010 Sie unterstützen, wenn ein Fehler auftritt oder wenn Sie einfach noch mehr Informationen benötigen? Diesen Fragen gehen wir in diesem Teil nach.

Anhang

Im Anhang finden Sie neben Informationen über Schulungen und MCP-Prüfungen auch ein paar Hintergrundinformationen über die Autoren, weiterführende Links im Internet sowie das Stichwortverzeichnis.

Unser Dank

Wenn drei Autoren ein IT-Fachbuch schreiben, geht das nicht wirklich ohne fremde Hilfe. Nein, keine Sorge, wir haben die einzelnen Kapitel nicht schreiben lassen. Aber bei einem überarbeiteten oder neuen Produkt wie Forefront TMG 2010 sind Rückfragen bei den Entwicklern unvermeidlich. Deshalb möchten wir uns an erster Stelle beim Forefront Threat Management Gateway-Team von Microsoft in Haifa und Redmond bedanken. Namentlich und besonders bei Jim Harrison und Tom Shinder.

Ohne unseren Verlag Microsoft Press und speziell unserem Lektor Florian Helmchen wäre dieses Buch nie veröffentlicht worden.

Ohne das Microsoft MVP-Programm wären wir sicherlich nicht seit vielen Jahren miteinander verbunden, was so ein Buchprojekt auch vereinfacht.

Ebenfalls bedanken wir uns bei allen Teilnehmern der Forefront User Group, den Newsgroups, Foren und anderen Veranstaltungen. Durch die zahlreichen Fragen und Anregungen konnten wir wieder viele Ideen für dieses Buch gewinnen. Unser Dank gilt auch Karsten Hentrup, welcher als Korrekturleser für unser Buch zur Verfügung stand und uns noch viele weitere Ergänzungen und Korrekturen geliefert hat Da wir sicherlich viele weitere Personen vergessen haben (was keine Absicht war!), bedanken wir uns ganz herzlich bei allen, die uns unterstützt haben.

Ganz besonders aber möchten wir uns bei Ihnen – dem Leser dieses Buchs – bedanken! Zu unseren letzten Büchern haben wir viel konstruktives Feedback bekommen. Wir haben uns bemüht, dieses bestmöglich umzusetzen und einzuarbeiten. Vielen Dank nochmals all denen, die sich bei uns gemeldet haben! Wer uns auch zu diesem Buch Feedback gibt, hat somit wieder die Chance, ein möglicherweise zu einem späteren Zeitpunkt folgendes Buch zu beeinflussen.

Wie können Sie Kontakt mit uns aufnehmen?

Uns ist durchaus klar, dass dieses Buch nicht alle Fragen rund um Forefront TMG 2010 beantworten kann. In unseren bisherigen Büchern haben wir daher immer angeboten, uns bei Fragen direkt eine E-Mail zu senden. Das haben unsere Leser auch fleißig genutzt. Teils für sehr willkommene Kritik, teils aber auch für Fragen zu komplexen Umgebungen und Problemen. Bitte haben Sie in solchen Fällen Verständnis dafür, dass wir Sie dann auf die öffentlichen Microsoft-Newsgroups und -Foren verweisen. Dort können solche Themen besser und umfangreicher diskutiert werden.

Selbstverständlich steht die E-Mail-Adresse *buch@msisafaq.de* noch immer zur Verfügung. Wir freuen uns über Ihre Kritik, Anregungen und Vorschläge.

Marc Grote

Christian Gröbner

Dieter Rauscher

Teil A

Grundlagen und Installation

Kapitel 1	Firewallgrundlagen	31
Kapitel 2	Windows Server 2008 R2 absichern	41
Kapitel 3	Einführung in die Forefront-Familie	53
Kapitel 4	Einführung in Forefront Threat Management Gateway 2010	71
Kapitel 5	Neuerungen in Forefront TMG 2010	77
Kapitel 6	Internetanbindung	87