Einleitung

Microsoft Forefront Threat Management Gateway 2010 – Das Handbuch, © 2010 Microsoft Press Deutschland, ISBN 978-3-86645-127-8

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.

Microsoft Forefront Threat Management Gateway 2010 – Das Handbuch, © 2010 Microsoft Press Deutschland, ISBN 978-3-86645-127-8

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 Inc.* 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 Klein	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