Kapitel 11

# Administration von Forefront TMG 2010



**In diesem Kapitel:**





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

In den vorherigen Kapiteln haben Sie ausführlich alles gelernt, um ein Forefront TMG 2010 erfolgreich zu planen und installieren. In diesem Kapitel geht es nun um die verschiedenen Möglichkeiten der Verwaltung.

# Verwaltung per Remotedesktop

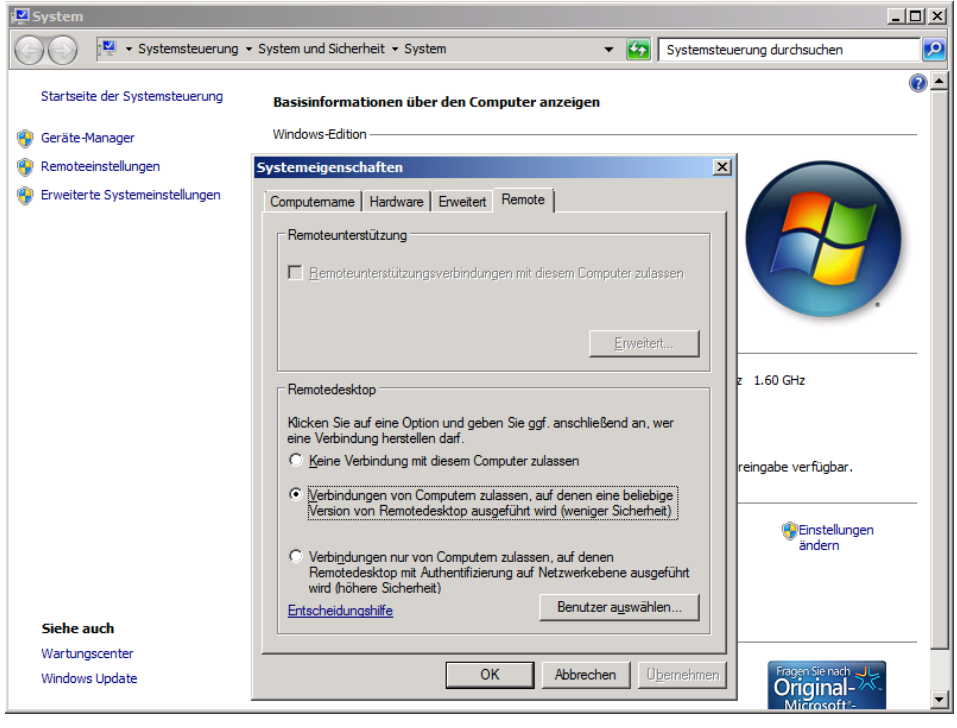
Bei Ihnen wird es sicherlich genauso sein wie bei Fabrikam Inc.: Die Server stehen in einem eigenen Serverraum und das Büro von Ihnen als Systemadministrator liegt nicht unmittelbar daneben. Vielleicht stehen Ihre Server ja auch in einem externen Rechenzentrum. Von daher können Sie nicht mal eben direkt an die Tastatur des Servers gehen, um Eingaben durchzuführen.

Deshalb werden Sie sicherlich schon lange alle Server statt über die direkt angeschlossene Kombination aus Tastatur, Maus und Bildschirm eher über Remotedesktop verwalten. Ist ja auch viel bequemer und spätestens seit Windows Server 2008 auch sehr zuverlässig.

Um Forefront TMG 2010 über die Remotedesktopfunktionalität von Windows Server 2008 R2 verwalten zu können, müssen sowohl auf dem Windows-Server als auch in Forefront TMG 2010 kleine Konfigurationsschritte durchgeführt werden.

Damit bei Windows Server 2008 R2 eine Remotedesktopverbindung hergestellt werden kann, muss diese Option in den Systemeigenschaften freigegeben werden. Sie finden diese in der in Abbildung 11.1 gezeigten Registerkarte *Remote*, indem Sie das Element *System und Sicherheit/System* in der Systemsteuerung öffnen. Alternativ genügt die Auswahl von *Eigenschaften* im Kontextmenü des Computers.

**Abbildg. 11.1** Benutzern erlauben, eine Remotedesktopverbindung herzustellen



Die folgenden Richtlinien helfen Ihnen bei der Auswahl der geeigneten Sicherheitseinstellung:

- Wählen Sie die Option *Keine Verbindung mit diesem Computer zulassen* aus, um zu verhindern, dass andere Benutzer mithilfe des Remotedesktops oder mit RemoteApp eine Verbindung mit Ihrem Computer herstellen.
- Wählen Sie die Option *Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird* aus, um Benutzern beliebiger Remotedesktop- oder RemoteApp-Versionen das Herstellen einer Verbindung mit Ihrem Computer zu ermöglichen. Diese Einstellung empfiehlt sich, wenn Ihnen die von anderen Benutzern verwendete Version der Remotedesktopverbindung nicht bekannt ist. Diese Einstellung ist jedoch weniger sicher, als die dritte Option.
- Wählen Sie die Option *Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird* aus, um Benutzern mit Computern, auf denen Remotedesktop- oder RemoteApp-Versionen mit Authentifizierung auf Netzwerkebene ausgeführt werden, das Herstellen einer Verbindung mit Ihrem Computer zu ermöglichen. Diese Option ist die sicherste Wahl, wenn Ihnen bekannt ist, dass die Benutzer, die eine Verbindung mit Ihrem Computer herstellen möchten, Windows 7 auf ihren Computern ausführen (unter Windows 7 verwendet der Remotedesktop die Authentifizierung auf Netzwerkebene).

Über die Schaltfläche *Benutzer auswählen* können Sie Benutzer oder Gruppen angeben, die sich per Remotedesktop mit dem Server verbinden dürfen. Der Domänenadministrator beziehungsweise der lokale Administrator hat automatisch Zugriff, sobald Remotedesktop erlaubt ist.

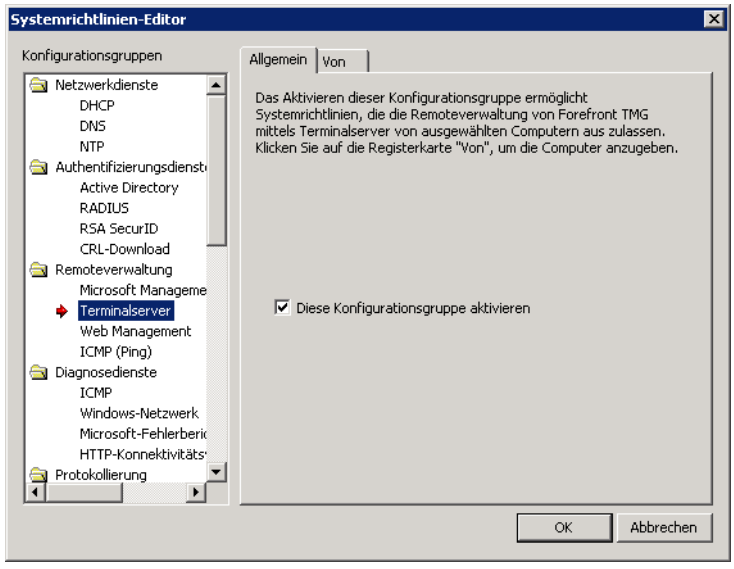
Nachdem nun der Windows Server soweit konfiguriert ist, können Sie sich der Konfiguration von Forefront TMG 2010 widmen.

Sie haben drei unterschiedliche Möglichkeiten, einem Clientcomputer per Remotedesktopprotokoll Zugriff auf den Forefront TMG 2010-Server zu gewähren:

1. Durch eine *Zugriffsregel*: Wenn Sie einem internen Client den Zugriff gewähren wollen, können Sie dafür eine entsprechende Zugriffsregel erstellen.
2. Durch eine *Serververöffentlichungsregel*: Wollen Sie einem externen Client den Zugriff gewähren, können Sie (wie in Kapitel 17 ausführlich beschrieben) eine Serververöffentlichungsregel verwenden.
3. Durch eine *Systemrichtlinie*: Die in den meisten Fällen idealere Lösung geht über eine Systemrichtlinie. Genauere Informationen und Vorteile einer Systemrichtlinie haben Sie bereits in Kapitel 9 erfahren. Nochmals kurz zur Erinnerung: Eine Systemrichtlinie hat Priorität vor den selbst erstellten Zugriffsrichtlinien und greift auch, wenn die Forefront TMG 2010-Dienste nicht gestartet sind.

Im weiteren Verlauf dieses Kapitels wird von der Konfiguration über eine Systemrichtlinie ausgegangen. Öffnen sie dazu die Forefront TMG 2010-Verwaltungskonsole und navigieren Sie zum Knoten *Firewallrichtlinie*. Wählen Sie aus dem Aufgabenbereich rechts den Punkt *Systemrichtlinie bearbeiten* (ganz unten) aus. Der in Abbildung 11.2 dargestellte Systemrichtlinien-Editor wird angezeigt. Suchen Sie den Punkt *Remoteverwaltung* und klicken Sie auf den Unterpunkt *Terminalserver.*

**Abbildg. 11.2** Der Systemrichtlinien-Editor




Auf der Registerkarte *Allgemein* können Sie diese Systemrichtlinie deaktivieren (standardmäßig ist sie aktiviert). Für dieses Beispiel muss die Systemrichtlinie jedoch aktiv bleiben. Gehen Sie stattdessen auf die Registerkarte *Von*. Hier können Sie, ähnlich wie bei einer normalen Zugriffsregel, angeben, für welche Quellen diese Regel zutreffen soll.

Direkt nach der Installation befinden sich folgende beiden Computergruppen als Quelle in dieser Systemrichtlinie:

- **Remoteverwaltungscomputer** Computer, die Forefront TMG remote verwalten können
- **Unternehmens-Remoteverwaltungscomputer** Vordefinierter Satz von Computern, die sämtliche Forefront TMG-Computer im Unternehmen remote verwalten dürfen. Diese Gruppe *Unternehmens-Remoteverwaltungscomputer* ist für Arrayinstallationen relevant.

Bearbeiten Sie den Computersatz *Remoteverwaltungscomputer* und fügen Sie alle Clients hinzu, die zu Verwaltungszwecken auf Forefront TMG 2010 zugreifen müssen. Dabei ist es unerheblich, ob ein Client eine interne oder externe IP-Adresse hat. Auch eine Mischung aus internen und externen Clients ist zulässig. Dadurch kann der Remotedesktop auch bestimmten externen Clients zugänglich gemacht werden. Beachten Sie jedoch dabei, dass bei Aufnahme eines externen Clients in den Computersatz *Remoteverwaltungscomputer* dieser auch alle anderen Zugriffsrechte erhält, die diesem Computersatz zugewiesen wurden. In den meisten Fällen ist das nicht gewünscht. Erstellen Sie daher für den externen Client ein eigenes Computerelement und fügen Sie das zusätzlich zu den *Remoteverwaltungscomputern* hinzu. Da Systemrichtlinien auch aktiv sind, wenn der Firewalldienst ausgefallen oder nicht gestartet ist, haben Sie dadurch normalerweise immer die Möglichkeit, sich mit dem Server zu verbinden. Schließen Sie anschließend den *Systemrichtlinien-Editor* und übernehmen Sie die Konfigurationsänderung.

Von Ihrem Administrationsclient können Sie nun die Anwendung *Remotedesktopverbindung* aufrufen und als Zielcomputer die IP-Adresse oder den Namen von Forefront TMG 2010 eingeben, um eine Remotedesktopverbindung aufzubauen.

Folgende Befehlszeilenoptionen stehen für eine Remotedesktopverbindung zur Verfügung:

```
MSTSC [<Verbindungsdatei>] [/v:<Server[:Port]>] [/admin] [/f[ullscreen]] [/w:<Breite> /
h:<Höhe>] [/public] | [/span] [/multimon] [/migrate] [/edit "Verbindungsdatei"]
"Verbindungsdatei" - Gibt den Namen einer RDP-Datei für die Verbindung an.
/v:<server[:Port]> - Gibt den Remotecomputer an, mit dem Sie eine Verbindung herstellen
möchten.
/admin - Stellt eine Verbindung mit der Sitzung zur Serververwaltung her.
/f - Startet Remotedesktop im Vollbildmodus.
/w:<Breite> - Gibt die Breite des Fensters "Remotedesktop" an.
/h:<Höhe> - Gibt die Höhe des Fensters "Remotedesktop" an.
/public - Führt Remotedesktop im öffentlichen Modus aus.
/span - Passt Höhe und Breite des Remotedesktops an den lokalen virtuellen Desktop an und
verteilt die Anzeige auf mehrere Monitore, falls erforderlich. Damit die Anzeige auf
mehrere Monitore verteilt werden kann, müssen die Monitore als Rechteck angeordnet werden.
/multimon - Konfiguriert das Bildschirmlayout der Remotedesktopsitzung so, dass es mit der
aktuellen clientseitigen Konfiguration identisch ist.
/edit - Öffnet die angegebene RDP-Verbindungsdatei zur Bearbeitung.
/migrate - Migriert die alten Verbindungsdateien, die mit Clientverbindungs-Manager
erstellt wurden, zu neuen RDP-Verbindungsdateien.
```



**TIPP** Mit dem Befehl *Mstsc.exe /admin* starten Sie eine Remotedesktopverbindung auf die Konsole von Windows Server 2008. Es handelt sich dabei um exakt dieselbe Konsole, die Sie auch verwenden, wenn Sie direkt mit Maus und Tastatur am Server arbeiten würden. Dies hat mehrere Vorteile:

- Sie sehen Anwendungs-Popups beziehungsweise Warnungen
- Sie können meist Anwendungen installieren, die mit dem Terminalservermodus nicht zurechtkommen

Sie können Anwendungen geöffnet lassen, wenn Sie zwischen echter Konsole und Remotedesktopverbindung wechseln.

**HINWEIS** Forefront TMG 2010 kann auch über eine Remotedesktopverbindung installiert werden. Während der Installation wird der Computer, von welchem die Installation erfolgt, dem Computersatz der *Remoteverwaltungscomputer* hinzugefügt und erlaubt somit auch einen Remotezugriff. Auch können die meisten Produktaktualisierungen direkt innerhalb einer Remotedesktopsitzung installiert werden, sofern der Zugang über eine Systemrichtlinie und nicht über eine Zugriffsregel eingerichtet wurde.

# Verwaltung mit der Forefront TMG 2010-Verwaltungskonsole

Zur Verwaltung und Konfiguration von Forefront TMG 2010 wird bei dem standardmäßigen Setup auch die Forefront TMG 2010-Verwaltungskonsole installiert. Wollen oder müssen Sie Forefront TMG 2010 von einem entfernten Arbeitsplatz aus verwalten, können Sie die Verwaltungskonsole innerhalb einer Remotedesktopsitzung öffnen, was zu Beginn dieses Kapitels beschrieben wurde. Dies ist grundsätzlich der empfohlene Weg.

Sie können die Forefront TMG 2010-Verwaltungskonsole auch an Ihrem Arbeitsplatzrechner installieren und dann direkt ohne Umweg über eine Remotedesktopverbindung Forefront TMG 2010 verwalten. Dazu muss in der Forefront TMG 2010-Konfiguration die Systemrichtlinie 2 *Remoteverwaltung mit MMC von ausgewählten Computern zulassen* angepasst werden. Öffnen Sie dazu wieder den *Systemrichtlinien-Editor* und wählen Sie unter *Remoteverwaltung* den Punkt *Microsoft Management Console (MMC)* aus. Aktivieren Sie das Kontrollkästchen auf der Registerkarte *Allgemein* und fügen Sie auf der Registerkarte *Von* den Computer oder Computersatz hinzu, von dem aus Sie die Forefront TMG 2010-Verwaltungskonsole nutzen möchten. Schließen Sie anschließend den *Systemrichtlinien-Editor* und übernehmen Sie die Konfigurationsänderungen.

Als Nächstes müssen Sie am Arbeitsplatzrechner die Forefront TMG 2010-Verwaltungskonsole installieren.

Verwenden Sie eine 32-Bit-Version von Windows 7, müssen Sie zuerst die Forefront TMG 2010-Verwaltungskonsole in 32-Bit herunterladen. Sie können nicht die 64-Bit-Version der Forefront TMG 2010-DVD verwenden. Diese können Sie nur auf einer 64-Bit-Version von Windows 7 installieren. Sie finden die 32-Bit-Version unter *http://go.microsoft.com/fwlink/?LinkId=179755*.

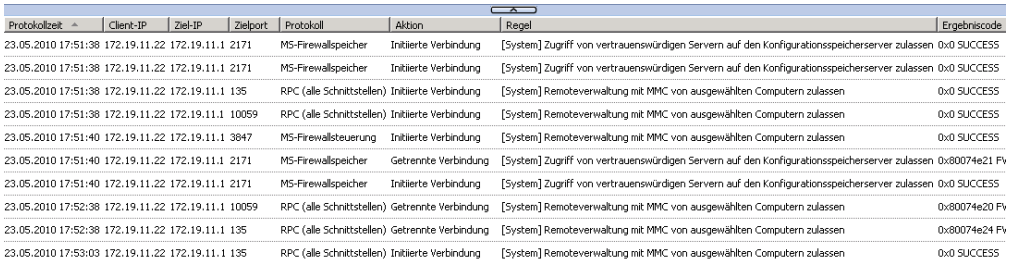
Starten Sie am Client das Setup von Forefront TMG 2010 entweder von DVD oder einer anderen Installationsquelle. Wählen Sie die Option *Installations-Assistenten ausführen*. Akzeptieren Sie den Lizenzvertrag und geben Sie die Produkt-Lizenznummer ein. Im Gegensatz zum regulären Forefront TMG 2010-Setup erkennt der Installations-Assistent automatisch, dass es eine Workstation ist. Daher wird nur die Option *Nur Forefront TMG-Verwaltung* angeboten. Anschließend werden die benötigten Dateien kopiert und nach kurzer Zeit ist die Installation fertiggestellt. Die kopierten Dateien sind Bestandteile der Forefront TMG 2010-Verwaltungskonsole und wurden standardmäßig in das Verzeichnis *C:\Programme\Microsoft Forefront Threat Management Gateway* kopiert. Zusätzlich wurde im Startmenü ein neuer Ordner *Microsoft Forefront TMG* angelegt, der das Element *Forefront TMG-Verwaltung* beinhaltet. Dies ist die normale Forefront TMG 2010-Verwaltungskonsole, wie sie auch am Forefront TMG 2010-Server selber vorhanden ist.

**HINWEIS** Sie können auf einem Computer gleichzeitig nur die Verwaltungskonsole einer ISA Server- beziehungsweise Forefront TMG 2010-Version installieren. Mehrere gleichzeitig sind nicht möglich.

Rufen Sie die Verwaltungskonsole erstmalig auf, müssen Sie eine Verbindung zu einem Forefront TMG 2010 herstellen. Geben Sie dazu im automatisch startenden Assistenten unter *Ort des Konfigurationsspeichers* mit tmg-muc.fabrikam.com den voll qualifizierten Domänennamen des Forefront TMG 2010-Computers an und klicken Sie auf die Schaltfläche *Weiter*. Bei einer Forefront TMG 2010-Standardversion ist der Konfigurationsspeicher immer auf demselben Server installiert. Im nächsten Schritt unter Anmeldeinformationen für den Konfigurationsspeicherserver müssen Sie ein Benutzerkonto angeben, welches berechtigt ist, Forefront TMG 2010 zu verwalten. Auf den nächsten Seiten lesen Sie, wie Sie solche Berechtigungen vergeben können. Auf der letzten Seite *Anmeldeinformationen für die Arrayverbindung* des Assistenten können Sie den oberen Punkt beibehalten und somit dieselben Anmeldeinformationen verwenden, wie zuvor schon für den Konfigurationsspeicherserver angegeben. Beenden Sie den Assistenten und anschließend steht Ihnen die gewohnte Forefront TMG 2010-Verwaltungskonsole am Client zur Verfügung.

In der Protokollierung sieht ein solcher Zugriff dann wie in Abbildung 11.3 dargestellt aus.

**Abbildg. 11.3** Protokollierung eines Zugriffs über die Forefront TMG 2010-Verwaltungskonsole



| Protokollzeit | Client-IP | Ziel-IP | Zielport | Protokoll | Aktion | Regel | Ergebniscode |
|---|---|---|---|---|---|---|---|
| 23.05.2010 17:51:38 | 172.19.11.22 | 172.19.11.1 | 2171 | MS-Firewallspeicher | Initiierte Verbindung | [System] Zugriff von vertrauenswürdigen Servern auf den Konfigurationsspeicherserver zulassen | 0x0 SUCCESS |
| 23.05.2010 17:51:38 | 172.19.11.22 | 172.19.11.1 | 2171 | MS-Firewallspeicher | Initiierte Verbindung | [System] Zugriff von vertrauenswürdigen Servern auf den Konfigurationsspeicherserver zulassen | 0x0 SUCCESS |
| 23.05.2010 17:51:38 | 172.19.11.22 | 172.19.11.1 | 135 | RPC (alle Schnittstellen) | Initiierte Verbindung | [System] Remoteverwaltung mit MMC von ausgewählten Computern zulassen | 0x0 SUCCESS |
| 23.05.2010 17:51:38 | 172.19.11.22 | 172.19.11.1 | 10059 | RPC (alle Schnittstellen) | Initiierte Verbindung | [System] Remoteverwaltung mit MMC von ausgewählten Computern zulassen | 0x0 SUCCESS |
| 23.05.2010 17:51:40 | 172.19.11.22 | 172.19.11.1 | 3847 | MS-Firewallsteuerung | Initiierte Verbindung | [System] Remoteverwaltung mit MMC von ausgewählten Computern zulassen | 0x0 SUCCESS |
| 23.05.2010 17:51:40 | 172.19.11.22 | 172.19.11.1 | 2171 | MS-Firewallspeicher | Getrennte Verbindung | [System] Zugriff von vertrauenswürdigen Servern auf den Konfigurationsspeicherserver zulassen | 0x80074e21 FV |
| 23.05.2010 17:51:40 | 172.19.11.22 | 172.19.11.1 | 2171 | MS-Firewallspeicher | Initiierte Verbindung | [System] Zugriff von vertrauenswürdigen Servern auf den Konfigurationsspeicherserver zulassen | 0x0 SUCCESS |
| 23.05.2010 17:52:38 | 172.19.11.22 | 172.19.11.1 | 10059 | RPC (alle Schnittstellen) | Getrennte Verbindung | [System] Remoteverwaltung mit MMC von ausgewählten Computern zulassen | 0x80074e20 FV |
| 23.05.2010 17:52:38 | 172.19.11.22 | 172.19.11.1 | 135 | RPC (alle Schnittstellen) | Getrennte Verbindung | [System] Remoteverwaltung mit MMC von ausgewählten Computern zulassen | 0x80074e24 FV |
| 23.05.2010 17:53:03 | 172.19.11.22 | 172.19.11.1 | 135 | RPC (alle Schnittstellen) | Initiierte Verbindung | [System] Remoteverwaltung mit MMC von ausgewählten Computern zulassen | 0x0 SUCCESS |



# Administrative Rollen zuweisen

Sie haben gerade gesehen, dass ein Benutzerkonto angegeben werden kann, um eine Remoteverwaltungskonsole zu verbinden. Dieses Konto muss kein Mitglied der Windows-Gruppen *Administratoren* oder *Domänen-Administratoren* sein. Es kann ein normales Benutzerkonto verwendet werden. Diesem Konto können Sie Forefront TMG 2010-Verwaltungsrollen in drei Stufen erteilen.

Folgende Rollen stehen zur Verfügung:

- **Forefront TMG-Arrayadministrator** Führen Sie jede Verwaltungsaufgabe über ein Forefront TMG-Array aus, einschließlich der Konfiguration von Regeln, der Anwendung von Netzwerkvorlagen und der Überwachung sowie dem Ausführen von Prozessen auf dem Forefront TMG-Server, für die hohe Berechtigungen erforderlich sind
- **Forefront TMG-Arrayprüfprogramm** Führen Sie alle Überwachungsaufgaben über ein Forefront TMG-Array aus, einschließlich der meisten Protokoll- und Alarmdefinitionskonfigurationen. Es gelten folgende Ausnahmen: Beim Veröffentlichen von Berichten kann kein anderes Benutzerkonto konfiguriert werden. Inhalte von Berichten können nicht angepasst werden. Außerdem können Forefront TMG-Arrayprüfprogramme die Forefront TMG-Konfiguration anzeigen.
- **Forefront TMG-Arrayüberwachungs-Prüfprogramm** Überwachen Sie grundlegende Server- und Netzwerkaktivitäten über einen Forefront TMG-Array. Die Forefront TMG-Konfiguration kann nicht angezeigt werden.

In Tabelle 11.1 finden Sie eine detaillierte Liste der einzelnen Berechtigungen.

**Tabelle 11.1** Rollen und die zugelassenen Aktionen

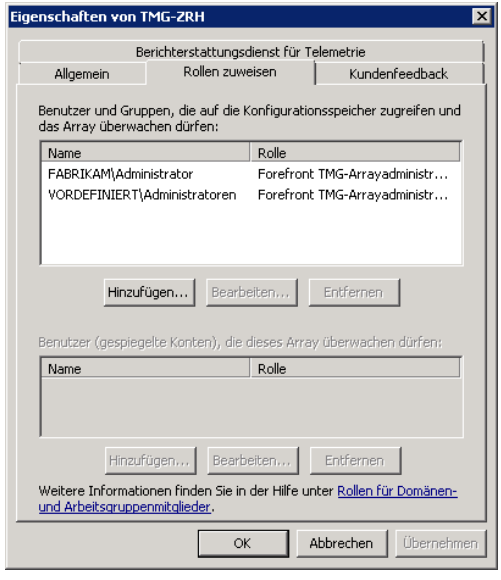
| Aktion | Administrator | Prüfprogramm | Überwachungs-prüfprogramm |
|---|---|---|---|
| Anzeigen der Übersicht, von Alarmen, Verbindungen, Sitzungen und Diensten | Zugelassen | Zugelassen | Zugelassen |
| Anerkennen und Zurücksetzen von Alarmen | Zugelassen | Zugelassen | Zugelassen |
| Anzeigen von Protokollinformationen | Zugelassen | Zugelassen | Nicht zugelassen |
| Erstellen von Alarmdefinitionen | Zugelassen | Nicht zugelassen | Nicht zugelassen |
| Erstellen von Berichten | Zugelassen | Zugelassen | Nicht zugelassen |
| Beenden und Starten von Sitzungen und Diensten | Zugelassen | Zugelassen | Nicht zugelassen |

**Tabelle 11.1** Rollen und die zugelassenen Aktionen *(Fortsetzung)*

| Aktion | Administrator | Prüfprogramm | Überwachungs-prüfprogramm |
|---|---|---|---|
| Anzeigen der Firewallrichtlinie | Zugelassen | Zugelassen | Nicht zugelassen |
| Konfigurieren der Firewallrichtlinie | Zugelassen | Nicht zugelassen | Nicht zugelassen |
| Konfigurieren des Caches | Zugelassen | Nicht zugelassen | Nicht zugelassen |
| Konfigurieren eines virtuellen privaten Netzwerks (VPN) | Zugelassen | Nicht zugelassen | Nicht zugelassen |
| Ausgleichen und Beenden der Netzwerklastenausgleich-Firewall oder des Webproxyservers mit Lastausgleich | Zugelassen | Zugelassen | Nicht zugelassen |
| Anzeigen der lokalen Konfiguration (in ADAM auf Arraymitglied) | Zugelassen | Zugelassen | Nicht zugelassen |
| Ändern der lokalen Konfiguration (in ADAM auf Arraymitglied) | Zugelassen | Nicht zugelassen | Nicht zugelassen |

**Profitipp** Es ist empfehlenswert, statt eines Benutzerkontos eine Gruppe zu verwenden. Prinzipiell sollten Berechtigungen nur auf Gruppenebene statt auf Benutzerebene vergeben werden. Dies betrifft nicht nur die Forefront TMG 2010-Konfiguration; vielmehr auch die Dateisystem- oder Messagingrechte in Exchange. Gruppen sind wesentlich flexibler handhabbar – ohne Aufwand kann ein Benutzer hinzugefügt werden, indem er der Gruppe hinzugefügt wird. Daraufhin verfügt dieser über sämtliche benötigten Rechte. Wenn jedes Mal Rechte für einen einzelnen Benutzer vergeben werden müssten, wäre der Verwaltungsaufwand zu hoch und es kann leichter passieren, dass vergessen wird, einem Benutzer bei Bedarf Rechte auch zu entziehen (zum Beispiel, wenn sich dessen Funktion geändert hat).

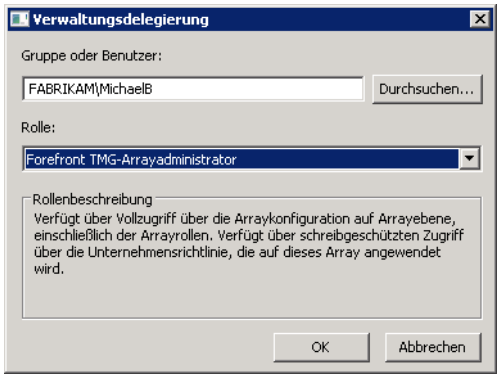
**Abbildg. 11.4** Registerkarte *Rollen zuweisen*



Um einer Gruppe oder einem Benutzer eine Rolle zuzuweisen, öffnen Sie die Forefront TMG 2010-Verwaltungskonsole und klicken mit der rechten Maustaste auf den Computerknoten *TMG-MUC* und wählen im zugehörigen Kontextmenü den Eintrag *Eigenschaften* aus. Öffnen Sie die zweite Registerkarte *Rollen zuweisen* (siehe Abbildung 11.4).

Klicken Sie auf die Schaltfläche *Hinzufügen*, um das Dialogfeld *Verwaltungsdelegierung* zu öffnen. Geben Sie hier die entsprechende Gruppe oder das Benutzerkonto an und weisen Sie, wie in Abbildung 11.5 dargestellt, die passende Rolle zu.

**Abbildg. 11.5** Weisen Sie Ihrem Benutzerkonto die Rolle als Administrator zu.






Beenden Sie nun die Rollenverwaltung und übernehmen Sie die Konfiguration. Jetzt können Sie auch von Ihrem Arbeitsplatzcomputer aus unter Ihrem Benutzerkonto die Forefront TMG 2010-Verwaltungskonsole starten und die Konfiguration einsehen oder verändern.

# Konfiguration exportieren und sichern

Die Exportfunktion von Forefront TMG 2010 ermöglicht es Ihnen, die gesamte Konfiguration oder nur einen Teil davon in eine XML-Datei zu schreiben und somit eine Sicherung der Einstellungen vorzunehmen. Die Sicherung der Konfiguration sollte auf jeden Fall ein wichtiger Punkt in der Planung für den Betrieb von Forefront TMG 2010 sein. Mittels einer Konfigurationssicherung können Sie im Notfall die gesamte Konfiguration auf einem neuen System wiederherstellen und somit den Betrieb zeitnah wieder aufnehmen. Der Export der gesamten Konfiguration kann auch dazu verwendet werden, um ein Versionsupgrade von ISA Server 2006 zu Forefront TMG 2010 durchzuführen und dadurch alle Einstellungen auf das neue System zu übertragen. Durch den Export von Teilen der Konfiguration können Sie zum Beispiel die Einstellungen der ISP-Redundanz zur Problemsuche durch einen Export auf ein Testsystem übertragen. Zusätzlich bietet der Export von Teilen der Konfiguration die Möglichkeit, bei Bedarf die ursprünglichen Einstellungen des exportierten Objekts wiederherzustellen, ohne dass Sie die gesamte Konfiguration erneut übernehmen müssen.

Die folgenden Objekte können in Forefront TMG 2010 exportiert werden:

- Die gesamte Konfiguration von Forefront TMG 2010
- Einzelne oder alle Systemrichtlinien
- Einzelne oder alle Firewallrichtlinien

- Einzelne Elemente der Toolbox (z.B. Computersätze, URL-Sätze …)
- Die gesamte Konfiguration des Webzugriffs (z.B. Richtlinien, Einstellungen, ...)
- Teile oder die gesamte E-Mail-Richtlinie
- Die VPN-Clientkonfiguration
- Einzelne oder alle Netzwerkeinstellungen (z.B. Netzwerke, Netzwerksätze)
- Webverkettungsregeln
- Einzelne Elemente oder alle Einstellungen der ISP-Redundanz
- Einzelne oder alle Konnektivitätsverifizierungen
- Cachekonfiguration (Cacheregeln, Inhaltdownloadaufträge)

Bei einem Export der gesamten Konfiguration von Forefront TMG 2010 werden alle aufgeführten Objekte exportiert. Der Export einzelner Objekte erfolgt entweder über das Kontextmenü des Objekts, über eine Aufgabe aus dem Aufgabenbereich oder über eine dafür gesondert vorhandene Schaltfläche.

**HINWEIS** Beachten Sie, dass bei einem Export der Firewallrichtlinien die Systemrichtlinien nicht enthalten sind. Diese müssen separat über das Kontextmenü des Knotens *Firewallrichtlinie* über den Eintrag *Alle Aufgaben/Systemrichtlinie/Systemrichtlinienregeln exportieren* exportiert werden.

# Gesamtkonfiguration exportieren

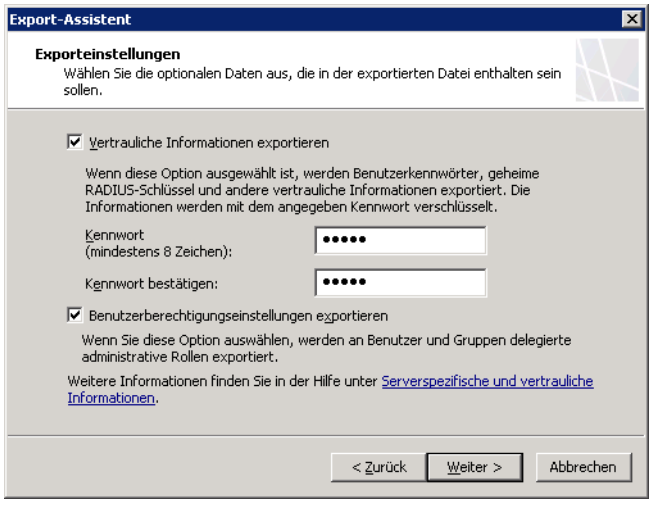
Zur Sicherung der Einstellungen oder Übertragung der Konfiguration auf einen anderen Server können Sie über die Exportfunktion von Forefront TMG 2010 die gesamte Konfiguration in eine XML-Datei exportieren. Anhand einer Sicherung der Einstellungen von Forefront TMG 2010 können Sie im Notfall problemlos auf eine Ersatzinstallation ausweichen, indem Sie die Konfigurationssicherung in diese importieren. Es werden dadurch alle Einstellungen aus der Konfigurationssicherung übernommen. Aus diesem Grund sollten Sie stets darauf achten, dass Sie immer eine aktuelle Sicherung der Konfiguration besitzen.

Nach der Umstellung von ISA Server 2006 auf Forefront TMG 2010 des Servers TMG-MUC am Standort München möchten Sie von der geänderten Konfiguration eine Sicherung erstellen, damit Sie im Notfall den Server schnell wiederherstellen können. Gehen Sie hierfür wie folgt beschrieben vor.

Öffnen Sie für den Export der Konfiguration zunächst die Verwaltungskonsole von Forefront TMG 2010 und markieren Sie den Knoten *Forefront TMG (TMG-MUC)*. Wählen Sie aus dem Kontextmenü des Knotens den Eintrag *Exportieren (Sichern)* aus, um den Assistenten für den Export der Konfiguration aufzurufen. Klicken Sie bei Anzeige der Willkommensnachricht auf die Schaltfläche *Weiter,* um mit dem Export zu beginnen. Im darauf folgenden Schritt erfordert der Assistent die Angabe über die Kontrollkästchen *Vertrauliche Informationen exportieren* und *Benutzerberechtigungseinstellungen exportieren,* ob Sie vertrauliche Informationen und Benutzerberechtigungen in diesem Export mit einschließen möchten. Durch den Export von vertraulichen Informationen werden Daten, wie zum Beispiel vorinstallierte Schlüssel (Preshared Keys, PSK) für IPsec-Standort-zu-Standort-Verbindungen oder geheime Schlüssel für die RADIUS-Kommunikation mit in die Exportdatei geschrieben. Zur Sicherheit müssen Sie hierfür ein Kennwort mit einer Mindestlänge von acht Zeichen in das Textfeld

*Kennwort* und zur Bestätigung nochmals in das Textfeld *Kennwort bestätigen* eintragen. Mithilfe des angegebenen Kennworts werden die vertraulichen Informationen in der Exportdatei verschlüsselt, damit diese nicht ohne Weiteres durch Dritte gelesen werden können.

**Abbildg. 11.6** Auswahl der Optionen für den Export






In Forefront TMG 2010 können Sie Benutzern bestimmte Rechte zuweisen, welche diese in der Verwaltungskonsole besitzen sollen. Durch den Export der Benutzerberechtigungen werden die von Ihnen konfigurierten delegierten Rechte an Benutzer und Gruppen ebenfalls in die Exportdatei geschrieben.

**ACHTUNG** Für eine vollständige Sicherung der Konfiguration müssen die beiden Optionen *Vertrauliche Informationen exportieren* und *Benutzerberechtigungseinstellungen exportieren* ausgewählt werden. Ansonsten können bei der Rücksicherung des Konfigurationsexports nicht alle Einstellungen übernommen werden, und Sie müssen diese von Hand nachpflegen.

Aktivieren Sie zur Erstellung einer Gesamtsicherung die beiden Kontrollkästchen *Vertrauliche Informationen exportieren* und *Benutzerberechtigungseinstellungen exportieren.* Vergeben Sie danach ein sicheres Kennwort zur Verschlüsselung der vertraulichen Informationen in den Textfeldern *Kennwort* und *Kennwort bestätigen.* Fahren Sie anschließend über die Schaltfläche *Weiter* mit dem Assistenten fort.

Der Assistent verlangt in diesem Schritt die Angabe des Speicherorts und eines Dateinamens für die Exportdatei. Diese können Sie entweder über die Schaltfläche *Durchsuchen* auswählen oder direkt in das Textfeld *Daten in dieser Datei speichern (vollständigen Pfad eingeben)* schreiben. Achten Sie bei der Auswahl des Speicherorts darauf, dass Sie die Exportdatei an einem sicheren Ort ablegen, der ausschließlich Administratoren zugänglich ist. Die vertraulichen Informationen werden zwar verschlüsselt in der Exportdatei hinterlegt, aber dennoch ist es möglich, Einstellungen wie Firewallrichtlinien im Klartext zu lesen. Zudem ist die Konfigurationssicherung von Forefront TMG 2010 nicht nur irgendeine weitere Textdatei auf dem Datenträger. Mittels NTFS-Berechtigungen können Sie im Dateisystem den Zugriff einschränken. Bei mobilen Datenträgern, wie USB-Sticks, ist es zu empfehlen, verschlüsselbare oder durch eine PIN geschützte Datenträger zu verwenden, da diese leicht verloren oder gestohlen werden können. Wählen Sie über die Schaltfläche *Durchsuchen* den

Speicherort für die Exportdatei aus und vergeben Sie einen aussagekräftigen Dateinamen. Klicken Sie anschließend auf die Schaltfläche *Weiter*. Bevor die Konfiguration durch den Assistenten exportiert wird, erhalten Sie eine Zusammenfassung der im Assistenten getroffenen Einstellungen angezeigt. Kontrollieren Sie diese nochmals und starten Sie danach den eigentlichen Export über die Schaltfläche *Fertig stellen*. Den Status des Exports können Sie im daraufhin angezeigten Fortschrittsbalken erkennen. Schließen Sie das Fenster über die Schaltfläche *OK*, sobald die Konfiguration erfolgreich exportiert wurde. Nach dem Durchlaufen des Assistenten und dem abschließenden Schreiben der Konfiguration in eine Datei sind Sie im Besitz einer aktuellen Sicherung der Einstellungen von Forefront TMG 2010. Die Sicherung kann zu einem späteren Zeitpunkt dazu genutzt werden, um die Konfiguration auf einen weiteren Server zu übertragen.

# Teile der Konfiguration exportieren

Nachdem Sie erfahren haben, wie Sie in Forefront TMG 2010 mithilfe der Exportfunktion eine Sicherung der gesamten Konfiguration erstellen können, behandelt dieser Abschnitt den Export von einzelnen Objekten der Konfiguration. Durch den Export von einzelnen Objekten, wie zum Beispiel einer Firewallrichtlinie, können Sie diese in einer anderen Installation wieder importieren. Häufig verwendete Firewallrichtlinien müssen somit nicht mehrmals einzeln erstellt werden, sondern können schnell über den Import der Konfiguration hinzugefügt werden. Der Export einer Teilkonfiguration kann auch dazu genutzt werden, eine Sicherung der Einstellungen für dieses Objekt zu erstellen. In Testumgebungen ist dies von Vorteil, wenn Sie Veränderungen an nur einem Objekt vornehmen wollen und zu einem späteren Zeitpunkt auf den ursprünglichen Zustand zurückkehren. Durch den Export der Einstellungen des Objekts müssen Sie nur dieses wieder herstellen und nicht die gesamte Konfiguration. Ein einzelner Export von Objekten kann auch dazu verwendet werden, die Einstellungen an Dritte zu übermitteln, damit diese im Bedarfsfall die Einstellungen des Objekts überprüfen können und Sie diesen nicht die gesamte Konfiguration überlassen müssen.

Wie bereits erwähnt, können Sie einzelne Objekte entweder über das Kontextmenü, eine Aufgabe im Aufgabenbereich oder über extra dafür vorhandene Schaltflächen exportieren. Im folgenden Beispiel wird die Konfiguration der ISP-Redundanz des Servers *TMG-MUC* am Standort München in eine Datei exportiert. Die Schritte des Exports gleichen denen eines Exports der Gesamtkonfiguration. Aus diesem Grund wird hier nicht mehr im Detail auf die einzelnen Schritte eingegangen.

Öffnen Sie für den Export der Konfiguration der ISP-Redundanz die Verwaltungskonsole des Servers *TMG-MUC* und navigieren Sie zum Knoten *Vernetzung*. Wechseln Sie danach zur Registerkarte *ISP-Redundanz*. In der Übersicht der konfigurierten Internetanbindungen könnten Sie eine einzelne Internetanbindung auswählen und über den Eintrag *Auswahl exportieren* des Kontextmenüs die Einstellungen dieser exportieren. Dabei würden nur die Einstellungen für die Internetanbindung exportiert werden. Sie beabsichtigen aber einen Export der gesamten Einstellungen der ISP-Redundanz. Klicken Sie hierzu im Aufgabenbereich auf die Aufgabe *Konfiguration der ISP-Redundanz exportieren*. Daraufhin startet wieder der Assistent für den Export. Klicken Sie im zunächst angezeigten Willkommensbildschirm auf die Schaltfläche *Weiter* und beginnen Sie mit der Angabe der Exporteinstellungen. Im Vergleich zum Export der Gesamtkonfiguration enthält dieser Schritt nur die Möglichkeit, vertrauliche Informationen zu exportieren, weil für einzelne Objekte keine Rechte in der Verwaltungskonsole von Forefront TMG 2010 delegiert werden können. Auch wenn mit ziemlicher Wahrscheinlichkeit im Export der Einstellungen der ISP-Redundanz keine vertraulichen Informationen enthalten sind, sollten Sie diese Funktion dennoch aktivieren, denn dadurch wird es später nur möglich sein, die Konfiguration wieder durch Eingabe des Kennworts zu importieren.

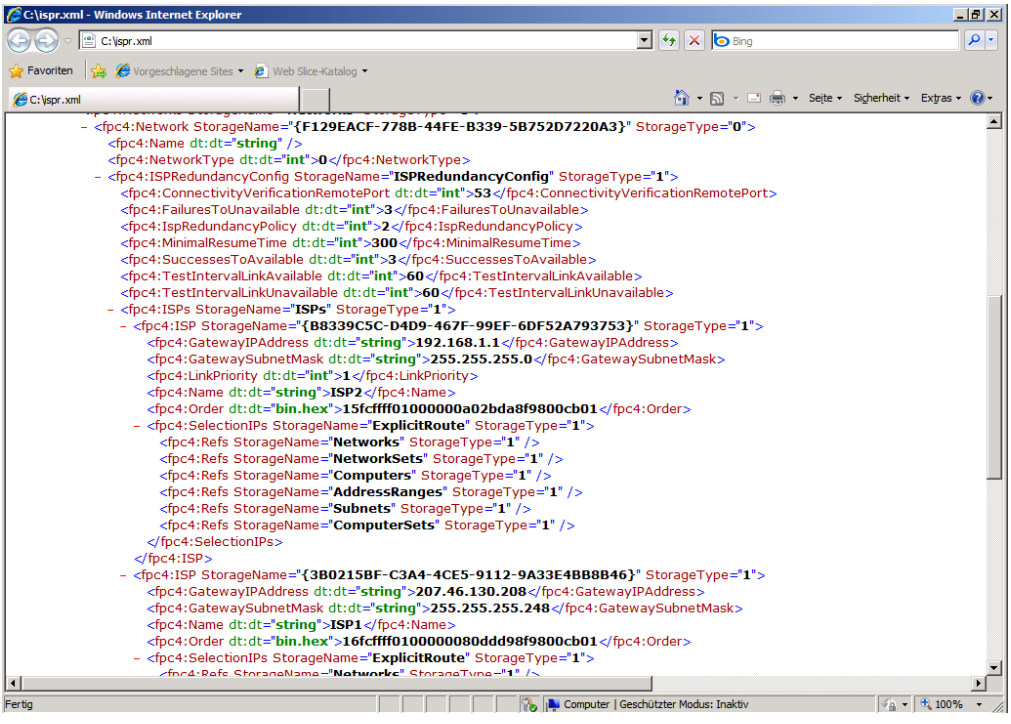
Dies bietet einen Schutz davor, dass exportierte Konfigurationen durch Dritte ohne Rücksprache einfach importiert werden. Exportieren Sie zum Beispiel die Client-VPN-Konfiguration oder ein IPsec-Standort-zu-Standort-Netzwerk, sollten Sie auf jeden Fall darauf achten, dass Sie die vertraulichen Informationen zusätzlich zu den Einstellungen in die Exportdatei schreiben lassen. Die VPN-Konfigurationen können nämlich vorinstallierte Schlüssel (Preshared Keys) enthalten, die ansonsten beim Export verloren gehen würden. Aktivieren Sie also das Kontrollkästchen *Vertrauliche Informationen exportieren* und vergeben Sie ein sicheres Kennwort in den Textfeldern *Kennwort* und *Kennwort bestätigen*. Fahren Sie anschließend über die Schaltfläche *Weiter* mit dem Assistenten fort.

Der nächste Schritt erfordert wieder die Angabe des Speicherorts und eines Dateinamens für die Exportdatei. Wählen Sie den Speicherort über die Schaltfläche *Durchsuchen* aus und vergeben Sie einen Dateinamen. Klicken Sie danach auf die Schaltfläche *Weiter*. Bevor der eigentliche Export ausgeführt wird, bekommen Sie durch den Assistenten die Einstellungen für den Export abschließend in einer Zusammenfassung angezeigt. Überprüfen Sie die angezeigten Einstellungen und starten Sie den Export über die Schaltfläche *Fertig stellen*. Daraufhin wird mit dem Export der Einstellungen begonnen. Schließen Sie das Fenster über die Schaltfläche *OK*, nachdem der Export erfolgreich durchgelaufen ist.

Die exportierte Datei können Sie einfach mithilfe eines Texteditors öffnen und sich die darin enthaltenen Einstellungen ansehen. Die Abbildung 11.7 zeigt ein Beispiel für eine exportiere Konfiguration der ISP-Redundanz.



**Abbildg. 11.7** Inhalt der Exportdatei mit den Einstellungen der ISP-Redundanz.



Wie Sie erkennen können, enthält das XML-Dokument die Einstellungen der ISP-Redundanz des Servers *TMG-MUC*. Zusätzlich können Sie dem XML-Dokument entnehmen, welche Root-DNS-Server für die Überprüfung der Verfügbarkeit der Internetanbindungen verwendet werden. Diese Einstellungen sind über die Verwaltungskonsole von Forefront TMG 2010 normal nicht einsehbar. Über die Exportdateien sind diese allerdings sichtbar. Es lohnt sich somit, gelegentlich einen Blick in die Exportdateien zu werfen.

Bewahren Sie die exportierte Konfiguration der ISP-Redundanz ebenfalls an einem sicheren Ort auf, damit diese vor Dritten geschützt ist und Sie diese bei Bedarf auch wiederfinden.

# Konfiguration per Skript exportieren

Aus Sicherheitsgründen sollten Sie in regelmäßigen Abständen eine Sicherung, vor allem eine Gesamtsicherung der Konfiguration von Forefront TMG 2010, erstellen. Leid eines jeden Administrators ist es jedoch, dass meist aus Zeitgründen vergessen wird, an eine regelmäßige Sicherung zu denken. Da Forefront TMG 2010 selbst keine Möglichkeit bietet, automatisiert eine Konfigurationssicherung zur erstellen, können Sie sich hier mit dem Skript aus Listing 11.1 behelfen.

**Listing 11.1** Skript zur automatisierten Konfigurationssicherung

```
Dim fileName
Dim WSHNetwork
Dim shareName: shareName = WScript.Arguments(0)
Dim xmldom : set xmldom = CreateObject("Msxml2.DOMDocument")
Dim fpc : set fpc = WScript.CreateObject("Fpc.Root")
Dim array : set array = fpc.GetContainingArray
set WSHNetwork = CreateObject("WScript.Network")
fileName=shareName & "\" & WSHNetwork.ComputerName & "-" &
Month(Now) & "-" & Day(Now) & "-" & Year(Now) & ".xml"
array.Export xmldom, 0
xmldom.save(fileName)
```

Übertragen Sie die Zeilen in einen Texteditor ihrer Wahl und speichern Sie anschließend die Datei unter dem Dateinamen **TMGBackup.vbs** ab. Übertragen Sie das Skript auf den Server mit Forefront TMG 2010 und kopieren Sie dieses in einen eigenen Ordner, wie zum Beispiel **C:\Skripts**. Testen Sie daraufhin die Funktion des Skripts. Öffnen Sie hierzu die Eingabeaufforderung über *Start/Alle Programme/Zubehör/Eingabeaufforderung* und wechseln Sie mit dem Befehl **cd c:\skripts** in den Ordner, in dem Sie das Skript abgespeichert haben. Starten Sie danach das Skript durch Eingabe folgender Befehlszeile **cscript TMGBackup.vbs c:\skripts** und bestätigen Sie dies über die ↵-Taste. Das Skript sollte nun die Konfiguration von Forefront TMG 2010 auslesen und in eine Datei mit dem Namen bestehend aus dem Servernamen und dem Erstellungsdatum in den Ordner *C:\Skripts* schreiben. Zwar ist es nicht sinnvoll, eine Konfigurationssicherung auf eine lokale Platte des Servers vorzunehmen, aber für einen Funktionstest des Skripts ist dies in Ordnung. Als Parameter für den Speicherort sollten Sie für die regelmäßige Sicherung der Konfiguration am besten eine Freigabe von einem anderen Server verwenden. Der Aufruf des Skripts würde dann zum Beispiel so aussehen:

```
cscript TMGBackup.vbs \\DC-MUC\TMGBackup
```

Dabei würde der Export der Konfiguration in die Freigabe *TMGBackup* auf dem Server *DC-MUC* erfolgen.

Damit Sie sich nicht jede Woche um die Ausführung des Skripts kümmern müssen, starten Sie dieses am besten über eine Aufgabe (Geplanter Task) in Windows Server 2008. Bevor Sie jedoch mit der Konfiguration der Aufgabe beginnen, erstellen Sie im Ordner *C:\Skripts* eine weitere Datei mit dem Inhalt *cscript c:\Skripts\TMGBackup.vbs \\DC-MUC\TMGBackup* und speichern Sie dieses unter dem Dateinamen *TMGBackup.cmd* ab. Hintergrund für die weitere Datei ist, dass sich dadurch die Erstellung der Aufgabe vereinfacht und Sie die Argumente somit nicht in der Aufgabe konfigurieren müssen. Nachdem Sie die zusätzliche Datei für den Aufruf des Backupskripts erstellt haben, müssen Sie eine Aufgabe für die automatische Ausführung konfigurieren.

Öffnen Sie hierzu die Aufgabenplanung aus dem Startmenü über *Start/Verwaltung/Aufgabenplanung.* Wählen Sie danach in der Verwaltungskonsole den Eintrag *Einfache Aufgabe erstellen* aus dem Menü *Aktion* aus. Vergeben Sie zu Beginn einen Namen für die neue Aufgabe im Textfeld *Name*, wie zum Beispiel *Sicherung der TMG-Konfiguration,* und klicken Sie anschließend auf die Schaltfläche *Weiter.* Der Assistent erfragt im nächsten Schritt das Zeitintervall, in dem die Aufgabe wiederholt werden soll. Im Normalfall sollte es ausreichen, eine wöchentliche Sicherung zu erstellen. Wählen Sie deshalb die Option *Wöchentlich* aus und fahren Sie über die Schaltfläche *Weiter* mit dem Assistenten fort. Neben dem Zeitintervall ist die Angabe des Zeitpunkts erforderlich, zu dem die Aufgabe ausgeführt werden soll. Stellen Sie diesen über die vorhandenen Felder in diesem Schritt ein und klicken Sie auf die Schaltfläche *Weiter.* Wählen Sie als Aktion die Option *Programm ausführen* aus und gehen Sie über die Schaltfläche *Weiter* zum nächsten Schritt über. Im Textfeld *Programm/Skript* verlangt der Assistent die Angabe der auszuführenden Datei. Wählen Sie über die Schaltfläche *Durchsuchen* die Datei *C:\Skripts\TMGBackup.cmd* aus. Das Textfeld *Argumente* kann leer bleiben, da Sie die Argumente für den Aufruf bereits im Windows-Befehlsskript (*TMGBackup.cmd*) hinterlegt haben. Fahren Sie danach über die Schaltfläche *Weiter* mit der Konfiguration fort. Zum Abschluss des Assistenten werden Ihnen die vorgenommenen Einstellungen für die Aufgabe in einer Zusammenfassung angezeigt. Überprüfen Sie diese und aktivieren Sie das Kontrollkästchen *Beim Klicken auf "Fertig stellen" die Eigenschaften für diese Aufgabe öffnen,* um weitere Einstellungen an der Aufgabe vorzunehmen. Beenden Sie im Anschluss den Assistenten über die Schaltfläche *Fertig stellen.*

In den Eigenschaften der Aufgabe müssen Sie noch zwei Einstellungen vornehmen, damit die Aufgabe regelmäßig ausgeführt und somit eine Sicherung der Konfiguration von TMG 2010 erstellt werden kann. Diese Einstellungen finden Sie auf der Registerkarte *Allgemein.* Als Erstes müssen Sie die Option *Unabhängig von der Benutzeranmeldung ausführen* auswählen, damit das Skript nicht nur ausgeführt wird, wenn ein Benutzer am Server angemeldet ist. Zudem sollten Sie das Skript mit erhöhten Privilegien ausführen, damit der Zugriff durch das Skript auf die Konfiguration von Forefront TMG 2010 und auf die Freigabe des Backup-Servers sichergestellt ist. Aktivieren Sie dazu das Kontrollkästchen *Mit höchsten Privilegien ausführen.* Die Konfiguration der Aufgabe ist danach abgeschlossen und Sie können das Fenster über die Schaltfläche *OK* schließen. Bevor Sie jedoch die Konfiguration der Aufgabe verlassen können, werden Sie noch nach den Anmeldedaten für die Aufgabe gefragt, die diese benötigt, um automatisch gestartet werden zu können. Achten Sie darauf, dass die für die Aufgabe hinterlegten Anmeldedaten sowohl Zugriff auf die Konfiguration von Forefront TMG 2010 als auch auf die Freigabe des Backupservers besitzen. Sollte dies nicht der Fall sein, wird die automatische Sicherung fehlschlagen. Überprüfen Sie auf jeden Fall die Ausführung der Aufgabe nach dem ersten geplanten Startzeitpunkt auf Fehler, damit Sie sicher sein können, dass durch die Aufgabe die Sicherungen richtig erstellt werden und testen Sie gegebenenfalls sogar einen Konfigurationsimport in ein Testsystem.

In diesem Abschnitt haben Sie erfahren, wie Sie mithilfe der Exportfunktion von Forefront TMG 2010 die gesamte Konfiguration beziehungsweise Teile der Konfiguration exportieren können. Abschließend wurde erläutert, wie Sie mit einem Skript eine automatisierte Sicherung der Konfiguration von Forefront TMG 2010 erreichen. Das Erstellen einer Sicherung ist nur ein Teil des Sicherungskonzepts für Forefront TMG 2010. Ein wichtiger Punkt des Sicherheitskonzepts sollte auch sein, dass Sie eine exportierte Konfiguration wieder in Forefront TMG 2010 erfolgreich importieren können.

# Konfiguration importieren und wiederherstellen

Über die Importfunktion von Forefront TMG 2010 können Sie eine gesamte Konfigurationssicherung wiederherstellen oder einzelne Konfigurationen übertragen, die von einem anderen Server exportiert wurden. Der Konfigurationsimport kann auf zwei unterschiedliche Arten ausgeführt werden. Die erste Möglichkeit ist das Hinzufügen der in der Exportdatei enthaltenen Einstellungen zur bestehenden Konfiguration. Die zweite Möglichkeit ersetzt die bestehende Konfiguration durch die in der Exportdatei enthaltenen Informationen, wodurch ein Übertragen einer gesamten Konfiguration oder eine Rücksicherung ermöglicht wird. Exportdateien von früheren Versionen, wie zum Beispiel von ISA Server 2006, werden beim Import automatisch auf das aktuelle Schema von Forefront TMG 2010 angepasst. Nachfolgend wird auf beide Arten wieder am Beispiel der Firma Fabrikam Inc. näher eingegangen.

## Konfiguration wiederherstellen

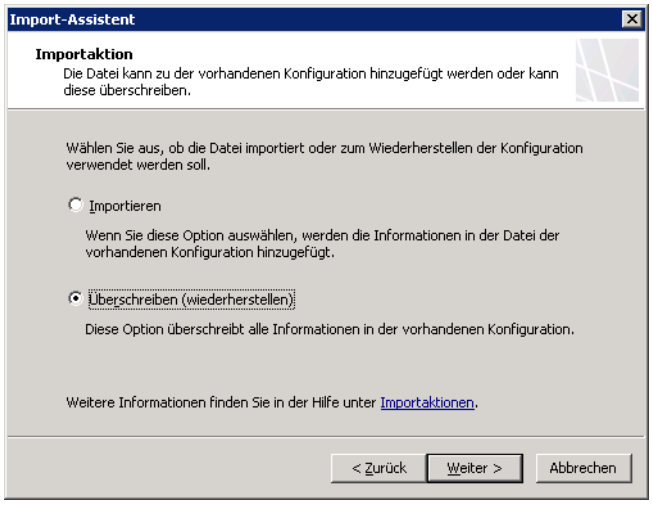
Beim Wiederherstellen einer Konfiguration über die Importfunktion wird die existierende Konfiguration von Forefront TMG 2010 durch die in der Exportdatei enthaltene Konfiguration komplett überschrieben. Dies ermöglicht das Übertragen einer Konfiguration von einem System auf das andere, was Sie zum Beispiel bei einem Update von ISA Server 2006 auf Forefront TMG 2010 benötigen, oder die Rücksicherung der gesamten Konfiguration, sollte Ihnen in der Konfiguration von Forefront TMG 2010 ein grober Fehler passiert sein. Sie haben bereits den Server *TMG-MUC* der Firma Fabrikam Inc. auf Forefront TMG 2010 aktualisiert und dabei das existierende Regelwerk von ISA Server 2006 ohne Veränderungen übernommen. Es ist Ihnen schon seit längerem ein Anliegen, das Regelwerk des Servers *TMG-MUC* einmal gründlich zu überarbeiten. Dies haben Sie aber bislang aus Zeitgründen noch nicht geschafft, und es ist Ihnen auch nicht möglich, dies während der Arbeitszeit zu erledigen, da Sie den Betrieb der Firma nicht stören möchten. Deshalb beschließen Sie, durch eine virtuelle Maschine die Netzwerkstruktur des Servers *TMG-MUC* nachzubilden und in dieser einen weiteren Server mit Forefront TMG 2010 zu installieren. In die vom Unternehmensnetzwerk getrennte virtuelle Maschine sichern Sie anschließend die Konfiguration von Forefront TMG 2010 in den Server *TMG-TEST* zurück und können diese problemlos überarbeiten.

Öffnen Sie zur Wiederherstellung einer Konfigurationssicherung die Verwaltungskonsole von Forefront TMG 2010 und navigieren Sie zum Knoten *Forefront TMG (TMG-TEST)*. Wählen Sie für die Rücksicherung einer Konfiguration aus dem Kontextmenü des Knotens *Forefront TMG (TMG-TEST)* den Eintrag *Importieren (wiederherstellen)* aus.

**HINWEIS** Für die Wiederherstellung einer Konfiguration ist es nicht erforderlich, dass der Server den gleichen Namen besitzt. Wichtig hingegen ist, dass die Netzwerkkonfiguration übereinstimmt und Sie alle Zertifikate, die Sie in Webserververöffentlichungen und Standort-zu-Standort-VPN-Verbindungen verwenden, ebenfalls auf diesem Server vorher importiert haben.

Die Rücksicherung einer Konfiguration wird im Forefront TMG 2010 mithilfe eines Assistenten durchgeführt, der Sie zu Beginn mit einer Willkommensnachricht begrüßt. Klicken Sie im Willkommensbildschirm auf die Schaltfläche *Weiter*. Im ersten Schritt ist es notwendig, über den Assistenten die Exportdatei mit der enthaltenen Konfiguration anzugeben, die wiederhergestellt werden soll. Wählen Sie diese über die Schaltfläche *Durchsuchen* aus oder tragen Sie den Dateinamen mit Pfadangabe im Textfeld *Dateiname* ein. Fahren Sie anschließend über die Schaltfläche *Weiter* mit dem Assistenten fort. Es folgt nun die Wahl der Importaktion für den Import.

**Abbildg. 11.8** Auswahl der Importaktion im Assistenten




Zur Auswahl stehen die beiden Optionen *Importieren* und *Überschreiben (wiederherstellen)*. Durch Auswahl der Option *Importieren* werden die Einstellungen aus der zu importierenden Datei der bestehenden Konfiguration hinzugefügt. Diese Aktion benötigen Sie zum Beispiel, wenn Sie Firewallrichtlinien der Konfiguration hinzufügen möchten. Dabei werden dem Regelwerk nur die in der Konfigurationsdatei enthaltenen Firewallrichtlinien hinzugefügt. Die restlichen Einstellungen, wie zum Beispiel die VPN-Konfiguration der ursprünglichen Konfiguration, bleiben erhalten. Anders verhält sich hier die Option *Überschreiben (wiederherstellen)*. Dabei wird die bestehende Konfiguration mit den in der Exportdatei enthaltenen Einstellungen komplett überschrieben. Wählen Sie zur Rücksicherung der Konfiguration von Forefront TMG 2010 des Servers *TMG-MUC* in den Server *TMG-TEST* die Option *Überschreiben (wiederherstellen)* aus. Klicken Sie anschließend auf die Schaltfläche *Weiter*.

Für die gesamte Wiederherstellung einer Konfiguration ist es wichtig, dass Sie serverspezifische Informationen, wie die Cachekonfiguration oder Informationen über verwendete SSL-Zertifikate, ebenfalls wiederherstellen. Eine Rücksicherung ist nur in Verbindung mit diesen Informationen vollständig. Damit diese Informationen importiert werden können, müssen sie in der Exportdatei

enthalten sein. Aktivieren Sie deshalb das Kontrollkästchen *Serverspezifische Informationen importieren.* Die Einstellungen zur Delegierung von Benutzerrechten für den Zugriff auf die Verwaltungskonsole von Forefront TMG 2010 kann ebenfalls über das Kontrollkästchen *Benutzerberechtigungseinstellungen importieren* mit zurückgesichert werden. Aktivieren Sie hierfür das Kontrollkästchen *Benutzerberechtigungseinstellungen importieren*, damit diese Informationen ebenfalls mit in die Konfiguration übernommen werden. Für eine gesamte Rücksicherung sind diese Informationen ebenso ein wichtiger Bestandteil. Klicken Sie nach Auswahl beider Optionen auf die Schaltfläche *Weiter.* Der nächste Schritt verlangt die Eingabe des Kennworts, anhand dessen die vertraulichen Informationen in der Exportdatei verschlüsselt wurden. Sofern Sie kein Kennwort beim Export vergeben haben, brauchen Sie hier auch kein Kennwort einzugeben. Wurde allerdings ein Kennwort vergeben und Sie überspringen diesen Schritt, wird der Import fehlschlagen, was Sie bei der Ausführung auch durch eine Fehlermeldung angezeigt bekommen. Für die Rücksicherung der vertraulichen Informationen ist es erforderlich, dass Sie ein Kennwort für den Import angeben. Tragen Sie das beim Export vergebene Kennwort in das Textfeld *Kennwort* ein und klicken Sie danach auf die Schaltfläche *Weiter.* Zum Abschluss des Assistenten bekommen Sie alle getroffenen Einstellungen nochmals in einer Zusammenfassung angezeigt. Überprüfen Sie diese und starten Sie danach die Rücksicherung der Konfiguration über die Schaltfläche *Fertig stellen.* Bevor die eigentliche Wiederherstellung der Konfiguration beginnt, erhalten Sie noch einen Warnhinweis, der Sie darauf aufmerksam macht, dass durch die Rücksicherung alle Einstellungen entfernt und überschrieben werden. Bestätigen Sie diesen Warnhinweis über die Schaltfläche *OK.* Daraufhin beginnt die Wiederherstellung der Konfiguration in den Server *TMG-TEST.* Anhand des Fortschrittsbalkens können Sie den Status der Aktion verfolgen. Schließen Sie das Statusfenster über die Schaltfläche *OK,* nachdem die Rücksicherung erfolgreich durchgeführt wurde. Übernehmen Sie abschließend die zurückgesicherte Konfiguration über die Schaltfläche *Übernehmen* in der Verwaltungskonsole von Forefront TMG 2010.

Es wurden somit ausnahmslos alle Einstellungen, wie zum Beispiel Alarmkonfigurationen, die VPN-Konfiguration oder Firewallrichtlinien inklusive Systemrichtlinien, in den Server *TMG-TEST* zurückgesichert. Dieser Server entspricht nun in etwa einem Klon des eigentlichen Servers. Dadurch, dass die Konfiguration exakt die gleiche ist, wie auf dem Server *TMG-MUC*, können Sie mit der Überarbeitung und Neugruppierung der Firewallrichtlinien beginnen und dies in aller Ruhe und ohne den Betrieb der Firma Fabrikam Inc. zu beeinträchtigen. Nachdem Sie mit der Überarbeitung der Konfiguration fertig sind, müssen Sie die Konfiguration von diesem Server wieder exportieren und in den Server *TMG-MUC* importieren.

## Konfigurationsteile importieren und wiederherstellen

Im vorigen Abschnitt haben Sie erfahren, wie Sie eine gesamte Konfiguration in Forefront TMG 2010 wieder herstellen können. Die Importfunktion erlaubt es auch, exportierte Teilkonfigurationen, wie zum Beispiel eine Firewallrichtlinie, in eine Installation zu importieren. Es werden dabei alle Regelelemente, wie Computer oder benutzerdefinierte Protokolle, die in der Firewallrichtlinie enthalten sind, ebenfalls erstellt und übernommen. Über den Import von Teilkonfigurationen können Sie somit auf einfache Weise häufig benötigte Konfigurationen auf andere Installationen von Forefront TMG 2010 übertragen, ohne diese jedes Mal neu erstellen zu müssen. Bei einem Import von Teilkonfigurationen wird auch nicht die gesamte Konfiguration überschrieben, sondern nur die in der Exportdatei enthaltenen Einstellungen. Wie Sie bei einem Import von Teilkonfigurationen vorgehen müssen, wird in diesem Abschnitt behandelt.

Der Administrator der Firma Contoso ist ein sehr guter Freund von Ihnen, mit dem Sie sich regelmäßig über aktuelle IT-Themen austauschen. Bei Contoso wird ebenfalls Forefront TMG 2010 als Firewall- und Webproxylösung verwendet. Für den Zugriff auf eine Anwendung im Internet hat der Administrator eine Firewallrichtlinie erstellt, die es ermöglichen soll, von internen Clients auf diese Anwendung zuzugreifen. Leider funktioniert der Zugriff trotz der erstellten Regel nicht. Er bittet Sie darum, dass Sie sich das Problem einmal anschauen und schickt Ihnen dazu die exportierte Firewallrichtlinie, die er für den Zugriff konfiguriert hat. Diese importieren Sie anschließend in Ihren Testserver *TMG-TEST* und testen den Zugriff auf diese Anwendung von einem Client.

Öffnen Sie hierzu die Verwaltungskonsole von Forefront TMG 2010 und navigieren Sie zum Knoten *Firewallrichtlinie*. Rufen Sie den Assistenten für den Import der Firewallrichtlinie aus dem Kontextmenü des Knotens *Firewallrichtlinie* über den Eintrag *Firewallrichtlinie importieren* auf. Daraufhin wird der Assistent für den Import aufgerufen, der Sie zu Beginn mit einer Willkommensnachricht begrüßt. Klicken Sie bei Erscheinen der Willkommensnachricht auf die Schaltfläche *Weiter*. Der erste Schritt erfordert wieder die Angabe der Exportdatei. Geben Sie diese entweder über die Schaltfläche *Durchsuchen* an oder tragen Sie diese direkt in das Textfeld *Dateiname* mit dem vollständigen Pfad ein. Klicken Sie danach auf die Schaltfläche *Weiter*. Erster Unterschied zur Wiederherstellung einer Konfiguration ist, dass beim Import einer Teilkonfiguration keine Benutzerzugriffseinstellungen importiert werden können, sondern nur serverspezifische Informationen. Diese sind aber auch nur in Konfigurationen, wie zum Beispiel einem Export von VPN-Clienteinstellungen enthalten. Für den Import der Firewallrichtlinie brauchen Sie demnach das Kontrollkästchen *Serverspezifische Informationen importieren* nicht zu aktivieren. Fahren Sie anschließend über die Schaltfläche *Weiter* mit dem Assistenten fort. Im nächsten Schritt bekommen Sie die abschließende Zusammenfassung für den Import der Firewallrichtlinie angezeigt. Das ist der zweite Unterschied zur Wiederherstellung einer Konfiguration. In dieser konnten Sie auswählen, ob Sie die Einstellungen hinzufügen oder überschreiben wollten. Anders ist dies beim Import von Teilkonfigurationen. Dabei werden die vorhandenen Einstellungen durch die in der Exportdatei enthaltenen prinzipiell überschrieben. Die restlichen Einstellungen bleiben hierbei allerdings unverändert. Ist ein Objekt, wie zum Beispiel eine Firewallrichtlinie noch nicht vorhanden, wird diese neu angelegt beziehungsweise hinzugefügt. Anhand einer internen ID (GUID) kann ermittelt werden, ob ein Objekt bereits existiert oder nicht.

Starten Sie den Import der Firewallrichtlinie per Klick auf die Schaltfläche *Weiter*. Daraufhin wird der Import der Firewallrichtlinie gestartet und Sie bekommen wieder das Statusfenster mit der Fortschrittsanzeige angezeigt. Schließen Sie dieses, nachdem der Import erfolgreich ausgeführt wurde, über die Schaltfläche *OK*. Übernehmen Sie danach die geänderten Einstellungen über die Schaltfläche *Übernehmen* in der Verwaltungskonsole von Forefront TMG 2010, damit die importierte Firewallrichtlinie aktiv wird. Sie probieren nun den Zugriff auf die Anwendung von einem internen Client über diese Firewallrichtlinie und stellen nach kurzer Zeit fest, dass dem Administrator der Firma Contoso ein Tippfehler im FQDN des in der Firewallrichtlinie enthaltenen Domänennamensatzes unterlaufen ist. Nachdem Sie diesen ausgebessert haben, funktioniert bei Ihnen der Zugriff. Die gewonnene Information teilen Sie per Telefon Ihrem Bekannten mit und dieser ist glücklich, dass Sie Ihm weiterhelfen konnten.

In diesem Abschnitt wurde anhand einer Firewallrichtlinie beschrieben, wie Sie einen Konfigurationsteilimport in Forefront TMG 2010 durchführen können. Der Aufruf des Assistenten für den Import ist nicht immer über ein Kontextmenü aufrufbar, sondern eventuell über zusätzliche Schaltflächen oder eine Aufgabe im Aufgabenbereich. Der restliche Verlauf des Assistenten gleicht aber den beschriebenen Schritten. Es sollte Ihnen somit nun möglich sein, jegliche Teilkonfigurationen in Forefront TMG 2010 zu importieren.

# Microsoft Forefront TMG Best Practices Analyzer Tool

Mit dem Microsoft Forefront TMG Best Practices Analyzer Tool (BPA) können Sie Ihre Konfiguration von Forefront TMG 2010 auf Schwachstellen und Fehlkonfigurationen überprüfen. Das Tool war bereits für die Vorgängerversionen ISA Server 2004 und ISA Server 2006 verfügbar. Inzwischen steht eine neue Version zur Verfügung, die in ihrer Datenbank zusätzlich zahlreiche Einstellungen für Forefront TMG 2010 enthält. Vom Produktteam wird die Datenbank in regelmäßigen Abständen mit neuen Einstellungen zur Überprüfung der Installation und Konfiguration von ISA Server 2004, ISA Server 2006 und Forefront TMG 2010 aktualisiert. Dadurch können Sie jederzeit mit einem Durchlauf des BPA feststellen, ob Sie in Ihrer Installation beziehungsweise Konfiguration von Forefront TMG 2010 eine Veränderung vornehmen sollten, die aufgrund von neuen Informationen in der Datenbank erkannt wurde.

## Microsoft Forefront TMG Best Practices Analyzer Tool installieren

Der BPA ist ein kostenloses Tool und kann von der Website *http://isabpa.com* heruntergeladen werden. Nach dem Herunterladen des MSI-Pakets kann sofort mit der Installation begonnen werden. Klicken Sie hierzu doppelt auf die Datei *tmgbpa.msi.* Daraufhin startet der Installations-Assistent, der Sie zunächst mit einem Willkommensbildschirm begrüßt. Klicken Sie hier auf die Schaltfläche *Next* und akzeptieren Sie im nächsten Schritt die Lizenzbestimmungen über die Option *I accept the terms in the License Agreement*. Fahren Sie anschließend mit der Installation über die Schaltfläche *Next* fort. Die Überprüfung auf Aktualisierungen des BPA ist ein wichtiger Bestandteil für den Betrieb, denn dadurch wird unter anderem die Datenbank mit den Überprüfungseinstellungen stets aktuell gehalten. Sie sollten dies über die Option *Yes. (Recommended)* zulassen. Andernfalls können Sie über die Option *No.* diese Funktion deaktivieren.

**HINWEIS** Beachten Sie, dass für die Aktualisierung des BPA der Zugriff des Servers auf die URL *https://www.microsoft.com/isaserver/code/isabpa/2.5/en* zugelassen werden muss. Diese Adresse müssen Sie gegebenenfalls in der Systemrichtlinie *Zugelassene Sites* hinzufügen.

Klicken Sie nach Auswahl der Aktualisierungsoption auf die Schaltfläche *Next.* Im nächsten Schritt werden Sie danach gefragt, ob Sie damit einverstanden sind, dass Informationen über die Ausführung des BPA an das *Customer Experience Improvement Program* gesendet werden dürfen. Mittels dieser Informationen können im BPA Fehler beseitigt und Funktionen erweitert werden. Die Informationen geben zum Beispiel Auskunft darüber, welche Hardware Sie verwenden oder welche Funktionen Sie im BPA nutzen. Es werden dabei keine vertraulichen Informationen weitergeben. Sofern Sie damit einverstanden sind, wählen Sie die Option *Participate in the Forefront TMG Best Practices Analyzer Tool Customer Experience Improvement Programm. (Recommended)* aus. Andernfalls deaktivieren Sie diese Funktion über die Option *I do not want to participate in this program at this time.* Klicken Sie danach auf die Schaltfläche *Weiter.* Im nächsten Schritt können Sie bereits mit der Installation über die Schaltfläche *Install* beginnen. Klicken Sie zum Abschluss der Installation auf die Schaltfläche *Finish.* Über

das Kontrollkästchen *Start the Forefront TMG Best Practices Analyzer Tool when the wizard closes* haben Sie die Möglichkeit, den BPA direkt nach Beenden des Installations-Assistenten zu starten. Alternativ können Sie den BPA aus dem Startmenü über *Start/Alle Programme/Microsoft Forefront TMG/TMG Tools/Forefront TMG Best Practices Analyzer* aufrufen.

# Konfiguration durch Microsoft Forefront TMG Best Practices Analyzer überprüfen

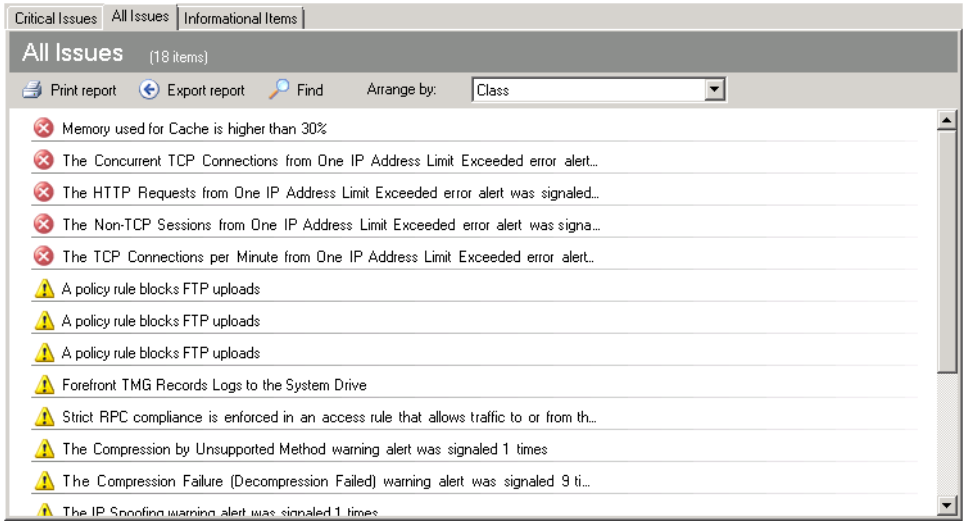
Nachdem Sie den Best Practices Analyzer (BPA) gestartet haben, überprüft dieser direkt nach dem Start, ob Aktualisierungen für die Version im Internet vorhanden sind. Hierzu müssen Sie allerdings bei der Installation des BPA zugestimmt haben. Sollte eine neuere Version zur Verfügung stehen, wird diese automatisch heruntergeladen und installiert. Im Anschluss können Sie über die Links *Select Options for a new scan* und *Select a Best Practices scan to view* auswählen, ob Sie eine neue Überprüfung durchführen oder ob Sie das Ergebnis eines vorigen Durchlaufs öffnen möchten. Klicken Sie zur Überprüfung der Konfiguration auf den Link *Select Options for a new scan.* Im Schritt *Start a scan* erfordert der BPA in den Textfeldern *Enter the scan label* eine Bezeichnung über die Überprüfung und im Textfeld *Enter the AD server* die Angabe eines Domänencontrollers. Ein vorhandener Domänencontroller wird bereits selbstständig ermittelt und als Vorschlag vorgegeben. Über das Listenfeld *Scan type* wählen Sie die Art der Überprüfung aus. Zur Auswahl stehen die folgenden Einträge:

- **Health check** Hierbei wird die Konfiguration nur auf Schwachstellen und Fehlkonfigurationen überprüft und diese anschließend in einem Bericht zusammengefasst dargestellt
- **All tasks** Diese Überprüfung führt neben der Überprüfung der Konfiguration zusätzlich einen verkürzten Export der Konfiguration aus, den Sie später über das Tool *ISAInfo* betrachten können. Nähere Informationen zu diesem Tool finden Sie in Kapitel 28. Diese Aktion benötigt etwas mehr Zeit für die Erstellung der Datei.

Wählen Sie im Listenfeld *Scan type* die Überprüfungsart aus, zum Beispiel *Health check,* und klicken Sie danach auf den Link *Start scan.* Nun werden alle Einstellungen gegen die Vorschläge aus der Datenbank überprüft. Anhand der Fortschrittsbalken der Kategorien *Hardware, ISA Configuration, ISA Installation* und *Operating System* sehen Sie, wie weit die Überprüfung fortgeschritten ist. Bei Auswahl der Überprüfungsart *All tasks* werden zusätzlich noch die Kategorien *Export TMG configuration* und *ISAInfo* mit aufgeführt. Nachdem alle Überprüfungen durchgelaufen sind, können Sie über den Link *View a report of the Best Practices scan* das Ergebnis anzeigen lassen. Wechseln Sie zum Bericht über den Link *View a report of the Best Practices scan.*

Der Bericht unterteilt sich in die drei Registerkarten *Critical Issues, All Issues* und *Informational Items.* Auf der Registerkarte *Critical Issues* finden Sie eine gefilterte Ansicht auf die durch den BPA gefundenen kritischen Probleme. Die Registerkarte *All Issues* hingegen enthält auch Warnungen, wie Sie in Abbildung 11.9 sehen können.

**Abbildg. 11.9** Bericht der Überprüfung durch den BPA




Auf der Registerkarte *Informational Items* finden Sie Informationen bezüglich der informellen Alarme in Forefront TMG 2010, der verwendeten Hardware, der Netzwerkkonfiguration und des Betriebssystems wieder. Die Ergebnisse sind nach dem Schweregrad sortiert. An oberster Stelle werden kritische Fehler aufgeführt und im Anschluss die Warnungen. Mit der Maus können Sie durch Auswahl des jeweiligen Eintrags die detaillierten Informationen zum erkannten Problem öffnen. Hier finden Sie Informationen darüber, was die Ursache und Auswirkung des erkannten Problems sind. Bei einigen aufgeführten Einträgen können Sie sich über den Link *Tell me more about this issue and how to resolve it* direkt zum dazugehörigen Kapitel in der Hilfe des BPA weiterleiten lassen.

Um stets eine Installation und Konfiguration von Forefront TMG 2010 zu betreiben, die sowohl sicher als auch fehlerfrei ist, sollten Sie den BPA in regelmäßigen Abständen ausführen. Dies hilft Ihnen dabei, einen reibungslosen Betrieb von Forefront TMG 2010 zu gewährleisten. Der BPA sollte somit bei keiner Installation von Forefront TMG 2010 auf dem Server fehlen.

# Zusammenfassung

In diesem Kapitel haben Sie die notwendigen Informationen erhalten, um erfolgreich Forefront TMG 2010 verwalten zu können. Dabei haben Sie die Vor- und Nachteile der einzelnen Möglichkeiten kennengelernt und sind nun in der Lage, die für Sie beste Lösung zu verwenden. Ergänzend dazu wurde Ihnen das wichtige Thema Sicherung und Wiederherstellung vorgestellt.

Im nächsten Kapitel wird auf die Konfiguration von Forefront TMG für spezielle Konfigurationen eingegangen und unter anderem die Konfiguration von Forefront TMG 2010 mit einer DMZ, als FrontEnd- und BackEnd-Firewall beschrieben und erklärt, warum die Installation von Forefront TMG 2010 auf einem Windows Server 2008 Domänencontroller nicht möglich ist.