# Verwenden von IPSec zum Sperren eines Servers

(Engl. Originaltitel: Using IPSec to Lock Down a Server)

*Steve Riley*

*Consultant, Microsoft Telecommunications Practice*

*Februar 2001*

Das IPSec-Richtlinienmodul von Windows 2000 bietet eine sehr effektive Möglichkeit zum Sichern einer Netzwerkschnittstelle. Bei einem Server, der nicht durch einen Firewall oder Router mit zuverlässigen Zugriffssteuerungslisten geschützt wird, ist das in diesem Artikel beschriebene Verfahren unbedingt erforderlich, um die Sicherheit des Servers zu gewährleisten. Und selbst, wenn ein Server durch eine oder mehrere Abwehrstufen geschützt ist, fügt dieses Verfahren eine weitere wirksame Stufe hinzu und verstärkt so die "umfassende Verteidigung" des Netzwerkes.

Sie erstellen keine IPSec-Sicherheitszuordnungen[1] zwischen dem Server und einem anderen Knoten, sondern legen mithilfe der IPSec-Schnittstelle und des Richtlinienmoduls fest, welche Protokolle in der Netzwerkschnittstelle des Servers zugelassen werden (wodurch alle anderen Protokolle blockiert werden). Diese Vorgehensweise ist wesentlich flexibler als die in den erweiterten Konfigurationsoptionen verfügbare TCP/IP-Filterung. Hier ist ein Vergleich der beiden Methoden:

| **Funktion** | **IPSec-Richtlinien** | **TCP/IP-Filterung** |
|---|---|---|
| Bereich | Bestimmte Adressen/Schnittstellen | Alle Schnittstellen des Servers |
| Quelladressen | Können Teil einer Richtlinie sein | Keine Möglichkeit zur Angabe |
| Neustart erforderlich | Nein | Ja |
| Reaktion auf blockierten Datenverkehr | Keine - eingehende Pakete werden verworfen; der Server ist nicht sichtbar | Zurücksetzen wird an den Client zurückgegeben |

Die Verwendung von IPSec-Richtlinien zum Sperren eines Servers erhöht Ihre Flexibilität. Sie können festlegen, welche Schnittstelle zu filtern ist und welche Quelladressen zugelassen werden (wenn diese Granularitätsebene benötigt wird). Darüber hinaus bieten IPSec-Richtlinien größere Sicherheit, indem blockierter Datenverkehr automatisch verworfen wird.

Für umfangreiches Bereitstellen von IPSec-Richtlinien und zum Einbeziehen der Richtlinienerstellung in einen automatisierten Servereinrichtungsprozess enthält das Windows 2000 Resource Kit das Befehlszeilenprogramm **IPSECPOL.EXE**. Es ermöglicht die skriptgesteuerte Erstellung von IPSec-Richtlinien. Im vorliegenden Dokument wird die Verwendung von **IPSECPOL.EXE** lediglich im Zusammenhang mit dem Sperren eines Servers erläutert. Ausführliche Informationen zu diesem Befehlszeilenprogramm finden Sie im Resource Kit.

# Strategie der umfassenden Verteidigung

Diese aus dem Militär bekannte Strategie lässt sich sehr gut auf die Informationssicherheit übertragen. Angesichts der Angriffe auf Informationen heutzutage reicht es aus folgenden Gründen nicht aus, sich auf einen einzigen Mechanismus für Netzwerk- und Hostsicherheit zu verlassen:

- Ein einziger Konfigurationsfehler ermöglicht einem Eindringling kompletten Zugriff auf das Netzwerk.
- Eine einzige Abwehrebene bietet nur geringen Widerstand gegen Angriffe, und einem Eingreifteam bleibt zu wenig Zeit zum Reagieren.
- Wenn versucht wird, alle Sicherheitsrichtlinien auf einer einzigen Ebene unterzubringen, kann dies zu unhandlichen Regelsätzen führen, die sich immer schwieriger verwalten lassen.

Wenn die Verantwortlichkeit für den Schutz auf mehrere Ebenen aufgeteilt wird, werden jeweils die folgenden Aspekte behandelt:

- Ein Konfigurationsfehler auf einer Ebene wird höchstwahrscheinlich auf einer anderen Ebene ausgeglichen.
- Mehrere Abwehrebenen verursachen einem Angreifer mehr Arbeitsaufwand - allein diese Tatsache wird von gelegentlichen Angriffen abschrecken. Außerdem bieten solche Abwehrebenen dem Eingreifteam die wertvollste Ressource: Zeit.
- Mehrere Sicherheitsstufen ermöglichen Ihnen das Erstellen von Richtlinien, die für jede Stufe geeignet sind. Dies vereinfacht den Konfigurationsaufwand.

Durch die umfassende Verteidigung können Änderungen auf flexible Weise berücksichtigt werden. Angenommen, Sie verfügen über ein DMZ-Netzwerk (Demilitarized Zone, Demilitarisierte Zone) mit einigen Webservern, einem Mailserver, einem Newsserver und einem DNS-Server. Mit einem automatisierten Prozess können Sie zudem die Rolle eines Servers problemlos ändern und so einen Webserver bei Bedarf umgehend zu einem Mailserver konvertieren. Wenn der Firewall anhand von Regeln steuert, welche Hosts Datenverkehr empfangen können, müssen Sie diese Regeln bei einer Änderung der Serverrolle anpassen. In umfangreichen Bereitstellungen können solche Wartungsaufgaben lästig werden. Konfigurieren Sie stattdessen den Firewall nur im Hinblick darauf, welche Protokolle - doch keine Quell- oder Zieladressen - im Netzwerk zugelassen werden. Ordnen Sie anschließend jedem Server eine IPSec-Richtlinie zu, durch die der auf dem Server eingehende Datenverkehr seiner Rolle entsprechend eingeschränkt wird. **IPSECPOL.EXE** vereinfacht diesen Vorgang erheblich. Sie können die Erstellung und Zuweisung der Richtlinie in den automatisierten Einrichtungsprozess einbeziehen. Immer, wenn Sie die Rolle eines Servers ändern müssen, erhält dieser automatisch die der neuen Rolle entsprechende IPSec-Richtlinie. Bei routinemäßigen Rollenänderungen sind keine Sicherheitsänderungen mehr erforderlich.

# Planen von Richtlinien

Bevor Sie mit dem Erstellen von IPSec-Richtlinien beginnen können, müssen Sie die besonderen Arten des Datenverkehrs für die einzelnen Server berücksichtigen. Am besten legen Sie sich zu diesem Zweck eine Liste an, die Ihnen beim Erstellen der Filter für die Richtlinie von Nutzen sein wird. Durch zu stark eingeschränkte Filter werden Anwendungsfehler verursacht; durch zu frei definierte Filter werden die Server unnötigerweise Angriffen ausgesetzt. Mit einem Dokument, das die erforderlichen Ports, Protokolle und Datenflussrichtungen für die einzelnen Serverrollen (oder Anwendungen) beschreibt, können Sie sicherstellen, dass Ihre Richtlinien für die vorgesehenen Zwecke geeignet sind.

Fertigen Sie ein Schema ähnlich dem nachstehenden an. Das Beispiel veranschaulicht einige Regeln für öffentlich verfügbare Web- und Mailserver. Ihre tatsächlichen Daten werden variieren. Dies gilt vor allem dann, wenn Sie beschließen, Regeln zur Einschränkung der Quelladressen des eingehenden Datenverkehrs bzw. der Zieladressen des ausgehenden Datenverkehrs zu implementieren.

| Rolle | Richtung | Von/zu | Schnittstellen-IP-Adresse | IP-Protokoll | TCP-/UDP-Port |
|---|---|---|---|---|---|
| Web - regulär | eingehend | alle | 131.107.1.1 | TCP | 80 |
| Web - SSL | eingehend | alle | 131.107.1.1 | TCP | 443 |
| SMTP | eingehend, ausgehend | alle, alle | 131.107.1.2 | TCP | 25 |
| POP3 - regulär | eingehend | alle | 131.107.1.2 | TCP | 110 |
| POP3 - SSL | eingehend | alle | 131.107.1.2 | TCP | 995 |
| IMAP4 - regulär | eingehend | alle | 131.107.1.2 | TCP | 143 |
| IMAP4 - SSL | eingehend | alle | 131.107.1.2 | TCP | 993 |

Wenn Sie das Schema fertig gestellt haben, können Sie mit dem Erstellen der IPSec-Richtlinien beginnen. IPSec-Richtlinien können im Active Directory gespeichert und über eine Gruppenrichtlinie den Computern zugewiesen werden.Trotzdem sollten die erstellten Sperrfilter unter Verwendung lokaler Richtlinien gespeichert werden, da diese auf bestimmte Computer zugeschnitten sind.

# Terminologie

Mithilfe der folgenden Begriffe können Sie IPSec-Richtlinien in Windows 2000 besser verstehen.

- *Filterliste.* Ports, Protokolle und Richtungen; löst eine Entscheidung aus, wenn der Datenverkehr mit den in der Liste festgelegten Kriterien übereinstimmt. Eine Liste kann mehrere Filter enthalten. Sie wird aus dem zuvor erstellten Schema abgeleitet.
- *Filteraktion.* Die erforderliche Reaktion, wenn der Datenverkehr mit einer Filterliste übereinstimmt. Im vorliegenden Fall treffen nur die Aktionen "Zulassen" und "Blockieren" zu.
- *Regel.* Direkter Zusammenhang einer Filterliste mit einer Filteraktion. Dient im Allgemeinen zum Festlegen von Parametern für die (hier nicht verwendete) IPSec-Sicherheitsaushandlung.
- *Richtlinie.* Eine Zusammenstellung von Regeln. Es kann jeweils nur eine Richtlinie aktiv ("zugewiesen") sein.

Nun können Sie mit dem Erstellen der IPSec-Richtlinie für einen Server beginnen. Zunächst verwenden Sie dazu die grafische Benutzeroberfläche. Später lernen Sie das Befehlszeilenprogramm im Resource Kit kennen.

# Erstellen der IPSec-Filterlisten und -Filteraktionen

Als ersten Schritt öffnen Sie die lokalen Sicherheitseinstellungen des Computers:

**Start | Programme | Verwaltung | Lokale Sicherheitsrichtlinie**

Über diese Verwaltungskonsole können Sie verschiedene Sicherheitsoptionen konfigurieren. Klicken Sie im linken Fensterausschnitt auf **IP-Sicherheitsrichtlinien auf lokalem Computer (IP Security Policies on Local Machine)**. Im rechten Fensterausschnitt werden die Standardrichtlinien von Windows 2000 angezeigt (die Sie hier nicht verwenden werden).

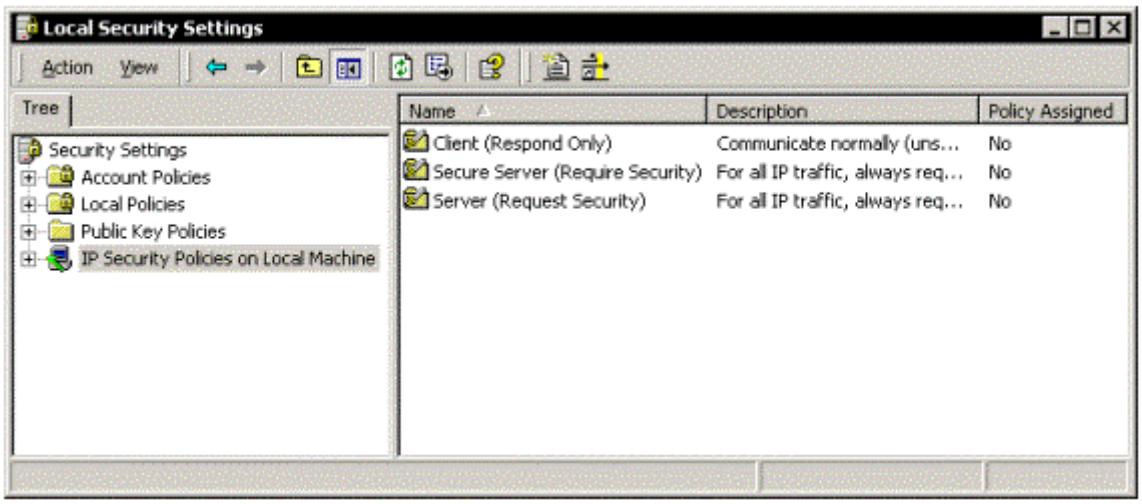


**Abbildung 1: Konsole "Lokale Sicherheitseinstellungen (Local Security Settings)"**

Klicken Sie mit der rechten Maustaste auf den rechten Fensterausschnitt. Oben im Menü gibt es zwei Optionen: **IP-Sicherheitsrichtlinie erstellen** und **IP-Filterlisten und Filteraktionen verwalten**. Da Sie vor dem Erstellen einer Richtlinie Listen und Aktionen benötigen, müssen Sie diesen Schritt zuerst ausführen. Klicken Sie auf die zweite Option, **IP-Filterlisten und Filteraktionen verwalten**.

Das Dialogfeld enthält zwei Registerkarten - eine für Filterlisten und eine für Filteraktionen. Auf der Registerkarte **IP-Filterlisten verwalten** werden die Standardfilterlisten von Windows 2000 angezeigt (die hier nicht verwendet werden).

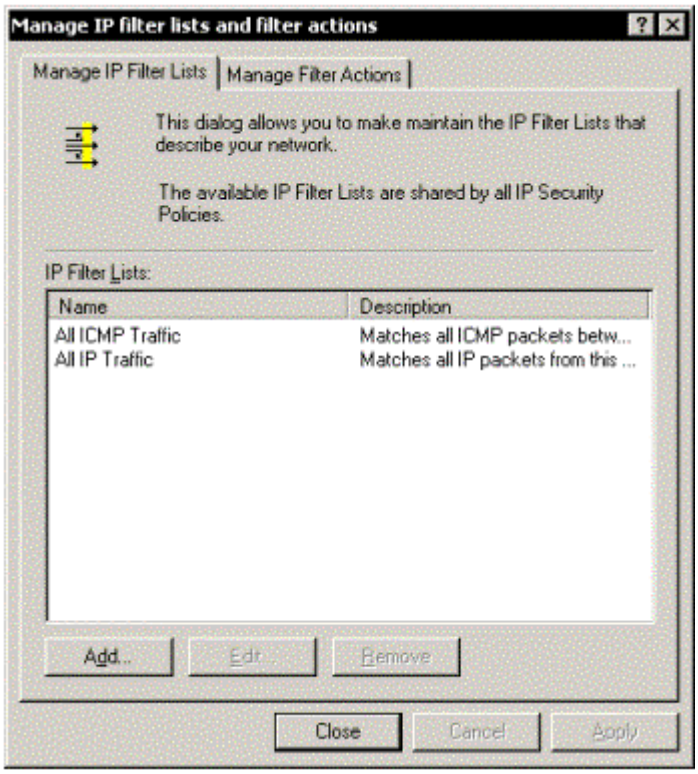


**Abbildung 2: Dialogfeld "IP-Filterlisten und Filteraktionen verwalten (Manage IP filter lists and filter actions)", Registerkarte "IP-Filterlisten verwalten (Manage IP Filter Lists)", mit Standardlisten**

Sie erstellen mindestens zwei Filterlisten:

- Eine Liste mit mindestens einem Filter, der dem Datenverkehr entspricht, der für den Server zugelassen werden soll. Abhängig von den auf dem Server ausgeführten Diensten können Sie mehrere Filter und mehrere Listen erstellen.
- Eine Liste, die allen eingehenden Protokollen und Ports entspricht. Der Grund für diese Vorgehensweise wird weiter unten erläutert.

Klicken Sie auf die Schaltfläche **Hinzufügen (Add)**, um eine neue Filterliste zu erstellen. Benennen Sie die Filterliste (z. B. **Eingehende Web-Protokolle [Inbound web protocols]**). In diesem Beispiel wird die Filterliste für einen Webserver gezeigt, der sowohl reguläre als auch SSL-Webfunktionen ausführt.

Klicken Sie im Dialogfeld **IP-Filterliste (IP Filter List)** auf die Schaltfläche **Hinzufügen (Add)**. Der IP-Filter-Assistent wird gestartet. Beantworten Sie die einzelnen Fragen des Assistenten anhand des zuvor erstellten Richtlinienplanes. Gezeigt wird nun weiterhin das Webserverbeispiel; dabei entspricht jede durch Aufzählungszeichen eingeleitete Zeile einer Seite im Assistenten:

- Die Quelladresse lautet: **Beliebige IP-Adresse (Any IP address)**.
- Die Zieladresse lautet: **Spezielle IP-Adresse (A specific IP address)**. Geben Sie die IP-Adresse der an das Internet angeschlossenen Schnittstelle ein. Wenn der Server nur eine einzige Schnittstelle aufweist, können Sie alternativ **Eigene IP-Adresse** wählen.
- Wählen Sie das entsprechende IP-Protokoll. Im vorliegenden Beispiel ist dies **TCP**.
- Auf der Seite **Port des IP-Protokolls** (die nur angezeigt wird, wenn Sie **TCP** oder **UDP** als Protokoll wählen) können Sie sowohl den Quell- als auch den Zielport festlegen. Die Standardeinstellungen lauten: **Von jedem Port** und **Zu jedem Port**. Zum Ändern des Zielports klicken Sie auf **Zu diesem Port** und geben die Portnummer der Anwendung ein. Im vorliegenden Beispiel ist dies **80**.
- Schließen Sie den Vorgang ab.

Führen Sie danach die gleichen Schritte im Assistenten aus, um einen weiteren Filter hinzuzufügen. Allerdings lautet der Zielport jetzt **443** (für HTTP über SSL). Die nachstehende Abbildung zeigt die fertige Filterliste.

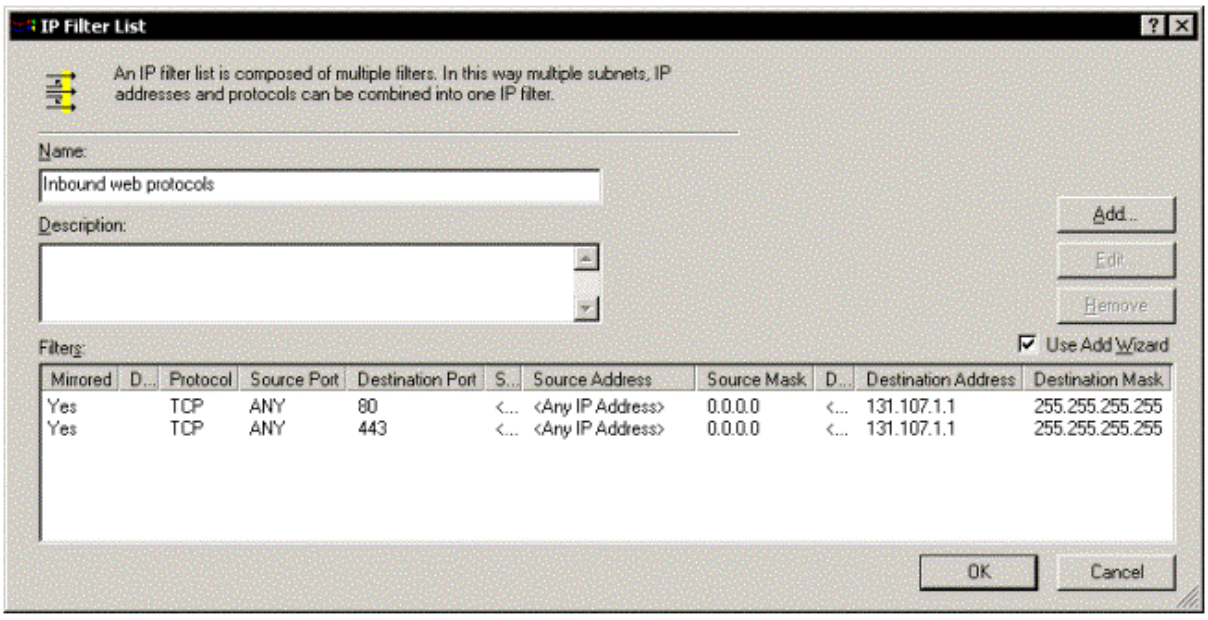


**Abbildung 3: Fertige IP-Filterliste für das Webserverbeispiel**

Als Nächstes müssen Sie eine Entscheidung treffen. Wenn Sie an einem nur für einen einzelnen Zweck eingesetzten Server arbeiten, wie z. B. dem Webserver in diesem Beispiel, sind jetzt alle erforderlichen Filter für den Server fertig erstellt. Verfügt der Server aber über mehrere Rollen, so können Sie entweder weitere Filter zur vorhandenen Filterliste hinzufügen, oder Sie können zusätzliche rollenspezifische Filterlisten erstellen. Rollenspezifische Listen sind flexibler, weil Sie Rollen problemlos in die Richtlinie einbeziehen oder aus ihr ausschließen können, ohne bestimmte Listen bearbeiten zu müssen.

Wenn Sie der vorhandenen Liste weitere Filter hinzufügen möchten:

- Klicken Sie auf die Schaltfläche **Hinzufügen (Add)**, und wiederholen Sie den Vorgang.

Wenn Sie die Liste fertig erstellt haben oder weitere Listen erstellen möchten:

- Schließen Sie das Dialogfeld **IP-Filterliste (IP Filter List)**. Damit kehren Sie zum Dialogfeld **IP-Filterlisten und Filteraktionen verwalten (Manage IP filter lists and filter actions)** zurück. Wenn Sie weitere Listen hinzufügen möchten, wiederholen Sie den gesamten Vorgang. (Wie oben erwähnt, sollte dies jedoch nur bei Servern, die für mehrere Zwecke eingesetzt werden, geschehen.)

***Filterliste "dem gesamten eingehenden Datenverkehr entsprechend".*** Sie müssen eine zusätzliche Filterliste erstellen, die dem gesamten Datenverkehr zur Schnittstelle entspricht. Die vorhandene Liste **Gesamter IP-Datenverkehr (All IP Traffic)** ist definiert als "dem gesamten von eigener IP-Adresse ausgehenden Datenverkehr entsprechend", was in diesem Fall nicht anwendbar ist. Erstellen Sie die korrekte Filterliste mit folgenden Schritten:

- Nennen Sie die Filterliste **Gesamter eingehender Datenverkehr (All inbound traffic)**.
- Beginnen Sie mit dem Hinzufügen eines Filters.
- Die Quelladresse lautet: **Beliebige IP-Adresse (Any IP address)**.
- Die Zieladresse lautet: **Bestimmte IP-Adresse (A specific IP address)**. Geben Sie die IP-Adresse der an das Internet angeschlossenen Schnittstelle ein. Wenn der Server nur eine einzige Schnittstelle aufweist, können Sie alternativ **Eigene IP-Adresse** wählen.
- Das IP-Protokoll lautet: **Beliebig**.
- Schließen Sie den Vorgang ab.

Diese Liste werden Sie in Kürze einer "Blockieraktion" zuordnen; mehr dazu später.

Wenn Sie Ihre Filterliste(n) fertig gestellt haben, klicken Sie auf die Registerkarte **Filteraktionen verwalten (Manage Filter Actions)**. Dort werden die Standardfilteraktionen von Windows 2000 angezeigt.

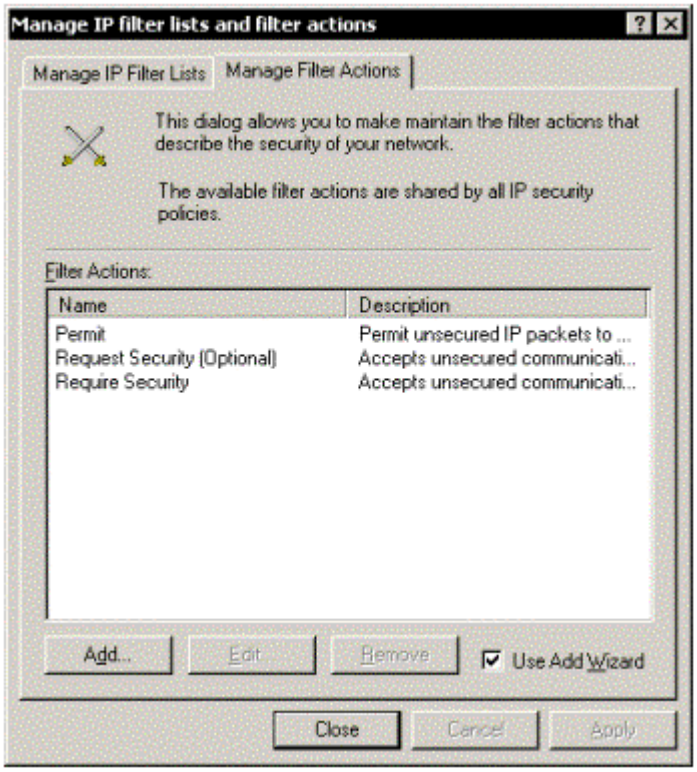


**Abbildung 4: Dialogfeld "IP-Filterlisten und Filteraktionen verwalten (Manage IP filter lists and filter actions)", Registerkarte "Filteraktionen verwalten (Manage Filter Actions)", mit Standardaktionen**

Eine der Aktionen lautet: **Zulassen (Permit)**. Wenn Sie die Regeln in Ihrer IPSec-Richtlinie einrichten, weisen Sie jeder der erstellten Filterlisten die Aktion **Zulassen** zu. Eine weitere Filteraktion wird benötigt: eine Blockieraktion. Diese sollten Sie jetzt mit folgenden Schritten erstellen:

- Klicken Sie auf die Schaltfläche **Hinzufügen (Add)**.
- Nennen Sie die Filteraktion **Blockieren**.
- Wählen Sie **Sperren** unter den allgemeinen Optionen aus.
- Schließen Sie den Vorgang ab.

Damit haben Sie alle erforderlichen Listen und Aktionen fertig gestellt. Schließen Sie das Dialogfeld **IP-Filterlisten und Filteraktionen verwalten (Manage IP filter lists and filter actions)**.

# Erstellen der IPSec-Richtlinie

Nachdem Sie die entsprechenden Filterlisten erstellt und eine Blockieraktion hinzugefügt haben, können Sie nun die IPSec-Richtlinie erstellen. Während dieses Vorgangs definieren Sie die Regeln, die die Listen mit Aktionen verknüpfen.

Klicken Sie in der MMC **Lokale Sicherheitseinstellungen (Local Security Settings)** mit der rechten Maustaste in den rechten Fensterausschnitt, und wählen Sie **IP-Sicherheitsrichtlinie erstellen**. Ein Assistent wird gestartet. Führen Sie die folgenden Schritte aus:

- Nennen Sie die Richtlinie **Paketfilter**.
- Deaktivieren Sie **Die Standardantwortregel aktivieren**. Eigentlich ist es unwichtig, ob dieses Kontrollkästchen aktiviert oder deaktiviert ist, da eingehende Verbindungen immer entweder zugelassen oder blockiert werden. Das Deaktivieren der Regel geschieht lediglich der Ordnung halber.
- Lassen Sie das Kontrollkästchen **Eigenschaften bearbeiten** aktiviert, und schließen Sie den Vorgang ab.

Die Richtlinie ist jetzt erstellt, enthält jedoch noch keine Regeln, wie Sie hier sehen können:

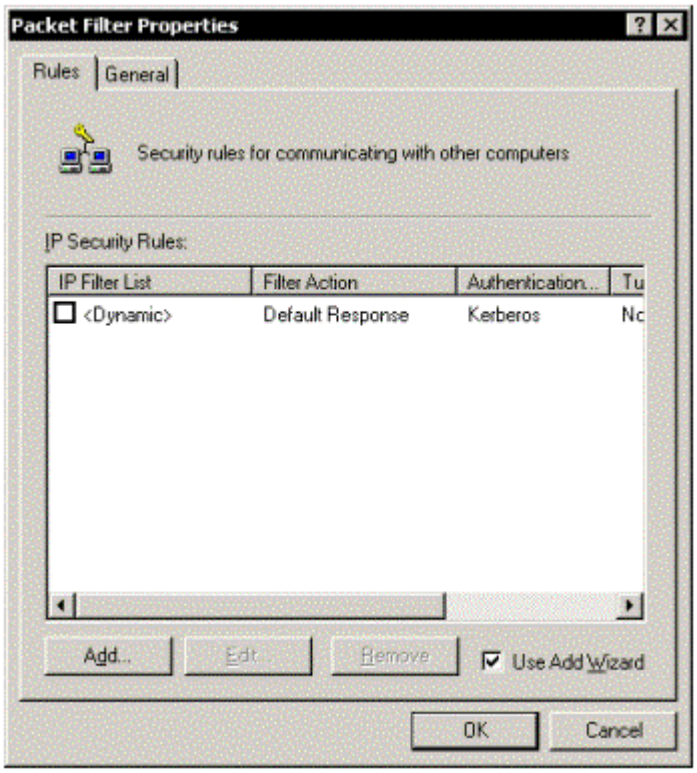


**Abbildung 5: Dialogfeld für die Eigenschaften der Richtlinie, mit Standardregeln**

Klicken Sie auf die Schaltfläche **Hinzufügen (Add)**, um mit dem Hinzufügen einer Regel zur Richtlinie zu beginnen. Führen Sie dazu folgende Schritte aus:

- Wählen Sie als Tunnelendpunkt **Diese Regel spezifiziert keinen Tunnel**.
- Der Netzwerktyp lautet **Alle Netzwerkverbindungen**.
- Die Authentifizierungsmethode lautet: **Windows 2000-Standard (Kerberos V5-Protokoll)**. Sie müssen Folgendes verstehen: Da durch diese Regel keine Sicherheit ausgehandelt wird, ist die Wahl der Authentifizierungsmethode ohne Belang. *Wenn Regeln den Datenverkehr lediglich blockieren oder zulassen, erfolgt keine Authentifizierung.* Durch das Beibehalten der Standardeinstellung (**Kerberos**) wird der Prozess der Regelerstellung jedoch vereinfacht.
- Wählen Sie die zuvor erstellte Filterliste. Im Zusammenhang mit diesem Beispiel wählen Sie **Eingehende Web-Protokolle (Inbound web protocols)**.
- Wählen Sie die Filteraktion **Zulassen (Permit)**. (Die nachstehenden Abbildungen veranschaulichen diesen und den vorhergehenden Schritt.)
- Schließen Sie den Vorgang ab.

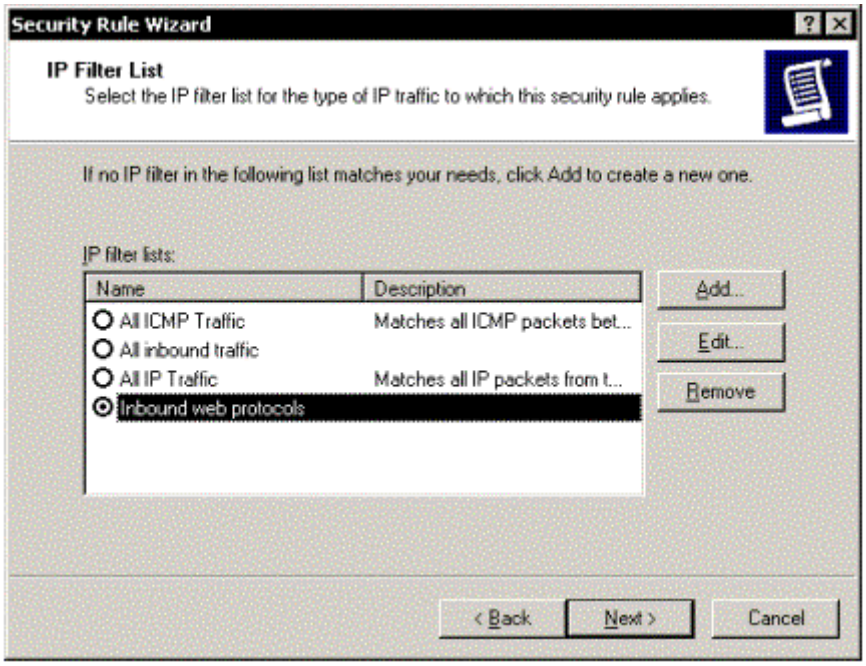


**Abbildung 6: Wählen der Filterliste entsprechend dem für den Server zugelassenen Datenverkehr**

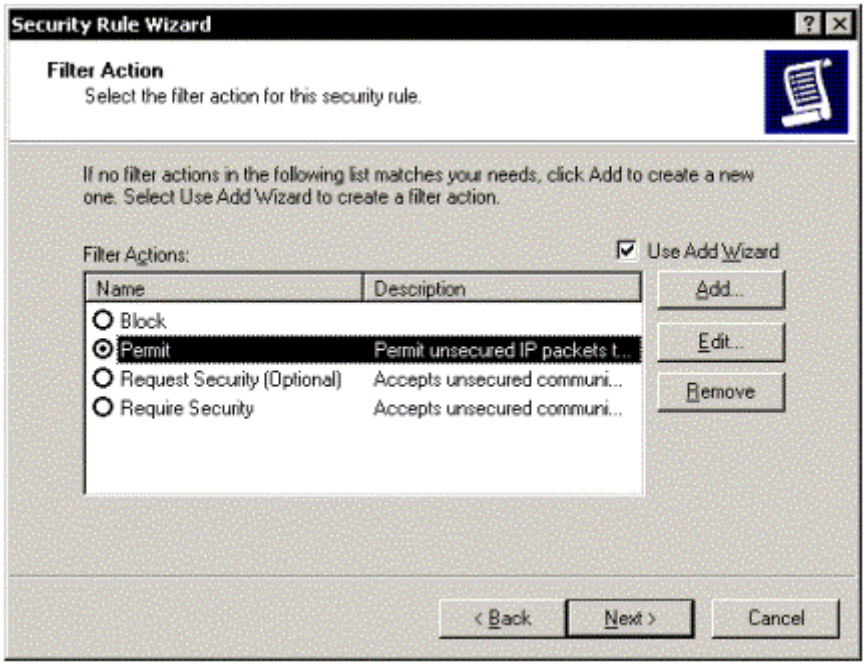


**Abbildung 7: Zuordnen der Aktion "Zulassen (Permit)" zu der zuvor ausgewählten Liste**

Falls Sie zusätzliche Filterlisten erstellt haben, wiederholen Sie den Vorgang, und ordnen Sie dabei die betreffende Filterliste jeweils der Aktion **Zulassen** zu.

Wiederholen Sie schließlich - als wichtigen Schritt - den Vorgang noch einmal, doch ordnen Sie diesmal die Filterliste **Gesamter eingehender Datenverkehr (All inbound traffic)** der Filteraktion **Sperren (Block)** zu. Da es im IPSec-Richtlinienmodul keinen Begriff "Standardverweigerung" gibt, brauchen Sie keine explizite Standardverweigerungsregel zu erstellen.

Nachdem Sie die Regeln fertig erstellt haben, sehen Ihre Richtlinieneigenschaften ähnlich wie hier aus:

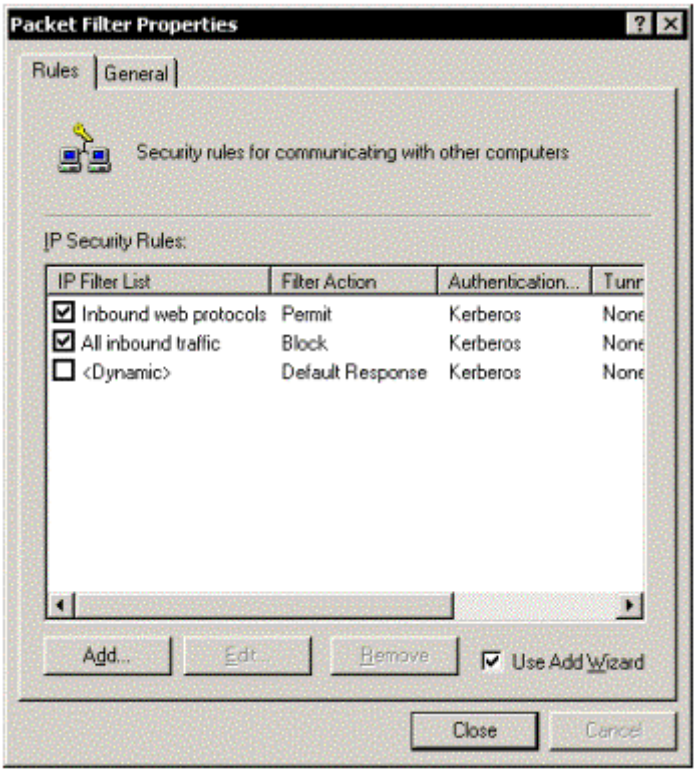


**Abbildung 8: Dialogfeld für die Eigenschaften der Richtlinie, mit fertig erstellten Regeln**

Schließen Sie das Dialogfeld der Richtlinieneigenschaften.

***Regelverarbeitung in IPSec-Richtlinien.*** Im Gegensatz zu typischen Firewall- oder Paketfilterregeln gibt es keine Möglichkeit, die Regelliste in einer IPSec-Richtlinie zu ordnen. Das Regelmodul ordnet dem Datenverkehr die Regeln der Übereinstimmung entsprechend zu. Wenn ein Paket mit mehr als einer Regel übereinstimmt, wendet das Modul die darauf am besten zutreffende Regel an. Im vorliegenden Fall entsprechen Pakete, die mit der Filterliste **Eingehende Web-Protokolle (Inbound web protocols)** übereinstimmen, gleichzeitig auch der Liste **Gesamter eingehender Datenverkehr (All inbound traffic)**. Da aber die erste Liste genauer zutrifft, entscheidet sich das Regelmodul für diese Liste. Deshalb wird der in **Eingehende Web-Protokolle (Inbound web protocols)** definierte Datenverkehr an den Server übergeben, während der gesamte andere Datenverkehr (gemäß der Definition in **Gesamter eingehender Datenverkehr (All inbound traffic)** blockiert wird. Ohne die Filterliste **Gesamter eingehender Datenverkehr (All inbound traffic)** und deren entsprechende Filteraktion **Sperren** würde die Richtlinie keine sinnvolle Aufgabe erfüllen!

# Aktivieren der IPSec-Richtlinie

Sie haben Filterlisten und Filteraktionen erstellt und diese den Regeln in einer IPSec-Richtlinie entsprechend zugeordnet. Als letzte Aufgabe müssen Sie nun noch die Richtlinie aktivieren, d. h. dem Server zuweisen. Es kann jeweils nur eine Richtlinie zugewiesen werden. Stellen Sie deshalb sicher, dass Ihre Filterlisten und Richtlinienregeln den gesamten Datenverkehr berücksichtigen, den der Server erwartungsgemäß verarbeiten wird.

So weisen Sie die Richtlinie zu

- Klicken Sie mit der rechten Maustaste auf die erstellte Richtlinie (in diesem Beispiel die Richtlinie **Paketfilter (Packet Filter)**, und wählen Sie **Zuweisen** aus dem Menü.

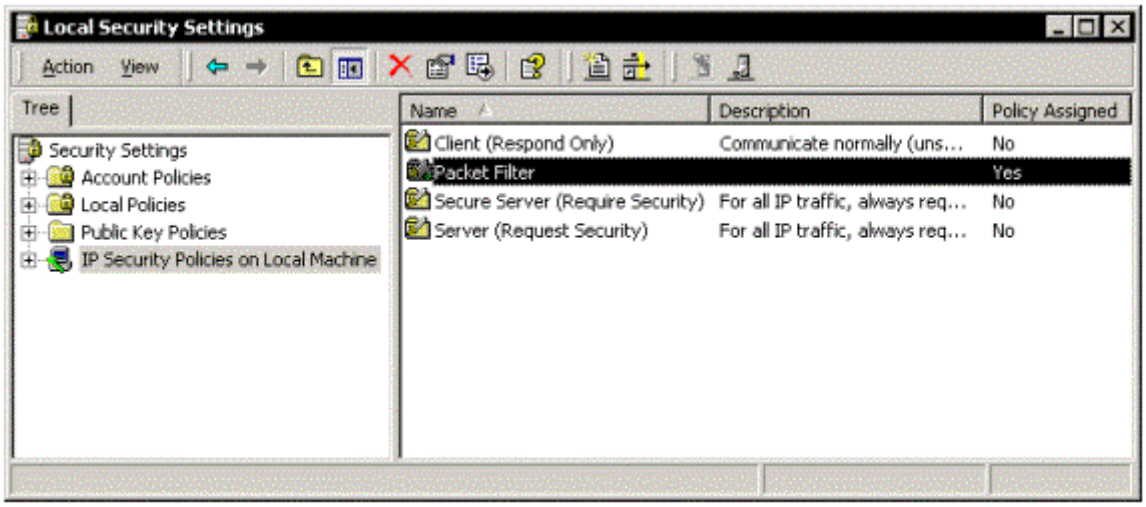


**Abbildung 9: Konsole "Lokale Sicherheitseinstellungen (Local Security Settings)", mit zugewiesener Richtlinie "Paketfilter (Packet Filter)"**

Die Richtlinie wird sofort zugewiesen, und das IPSec-Modul beginnt mit der Paketverarbeitung gemäß den Regeln der Richtlinie. Sie brauchen den Server nicht neu zu starten.

# Skriptgesteuertes Erstellen von Richtlinien mit "IPSECPOL.EXE"

Im Windows 2000 Resource Kit ist das Befehlszeilenprogramm **IPSECPOL.EXE** enthalten, mit dem Sie IPSec-Richtlinien erstellen, zuweisen und löschen können. **IPSECPOL.EXE** ist äußerst flexibel und in der Lage, dynamische und statische Richtlinien im Active Directory sowie in lokalen und Remoteregistrierungen zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation im Resource Kit. Im Rahmen dieses Beispiels erstellen Sie nun statische Richtlinien in der Registrierung des lokalen Computers.

**IPSECPOL.EXE** verfügt über mehrere Parameter, und die Syntax ist auf den ersten Blick möglicherweise schwierig zu verstehen. Wenn Sie jedoch die im Folgenden vorgestellten Beispiele ausführen, können Sie - mit nur drei Befehlen - die gesamte Konfiguration aus den vorhergehenden Beispielen der grafischen Benutzeroberfläche duplizieren. Wenn Sie möchten, können Sie die Microsoft Management Console (MMC) öffnen und deren Anzeige nach jedem Befehl aktualisieren, um das erwartungsgemäße Ausführen des Befehls zu überprüfen. Beginnen Sie nun mit dem Vorgang.

Der erste Befehl erstellt eine neue Richtlinie, fügt ihr eine Regel hinzu und fügt der Regel dann zwei Filterlisten und eine Filteraktion hinzu:

```
ipsecpol -w REG -p "Packet Filter" -r "Inbound web protocols"
-f *+131.107.1.1:80:TCP -f *+131.107.1.1:443:TCP -n PASS
```

Dieser Befehl ist für Druckzwecke in zwei Zeilen wiedergegeben; geben Sie ihn aber als eine einzige Zeile ein. Die Parameter bedeuten:

- **–w REG –** Schreiben einer statischen Richtlinie in die Registrierung. Dies entspricht exakt der Verwendung der MMC.
- **–p "Packet Filter" –** Erstellen einer Richtlinie namens "Packet Filter".
- **–r "Inbound web protocols" –** Erstellen einer Regel namens "Inbound web protocols".
- **-f *+131.107.1.1:80:TCP –** Hinzufügen eines Filters, in dem die Elemente **`*`** eine beliebige Quelladresse und einen beliebigen Port, **`131.107.1.1:80`** die Zieladresse (die Adresse des Servers) und einen bestimmten Port sowie **`:TCP`** das Protokoll festlegen und das Element **+** angibt, dass der Filter gespiegelt wird.
- **–f *+131.107.1.1:443:TCP –** Identisch mit dem vorherigen Befehl, außer dass der Zielport **`443`** lautet.
- **–n PASS –** Durchlassen des Datenverkehrs ohne Aushandeln der Sicherheit.

Bei den Werten der Parameter **`–w`**, **`–f`** und **`–n`** muss die Groß-/Kleinschreibung beachtet werden; verwenden Sie nur Großbuchstaben!

Sie können beliebig viele Filter einbeziehen. Wenn auf einem Server mehrere Dienste ausgeführt werden, sollten Sie für jede Klasse von Filtern einen separaten **IPSECPOL.EXE**-Befehl verwenden. Dies wurde weiter oben im Zusammenhang mit rollenspezifischen Filterlisten erläutert. Beispielsweise lässt der folgende Befehl eingehende Verbindungen an die Ports 110, 995, 143, 993 und 25 sowie ausgehende Verbindungen zu einer beliebigen Adresse an Port 25 zu:

```
ipsecpol –w REG –p "Packet Filter" –r "Inbound/outbound mail"
–f *+131.107.1.1:110:TCP –f *+131.107.1.1:995:TCP
–f *+131.107.1.1:143:TCP –f *+131.107.1.1:993:TCP
–f *+131.107.1.1:25:TCP –f 131.107.1.1+*:25:TCP
–n PASS
```

(Der letzte Filter, **–f 131.107.1.1+*:25:TCP**, sieht etwas anders aus. Er lässt zu, dass ausgehender Datenverkehr von der eigenen Adresse des Servers an einem beliebigen Port zu einem beliebigen Server an Port 25 übertragen wird. Dieser Filter ermöglicht dem Server das Initiieren ausgehender SMTP-Verbindungen ins Internet.)

Der nächste Befehl erstellt die allgemeine Regel, die auf den gesamten Datenverkehr zutrifft und diesen blockiert:

```
ipsecpol –w REG –p "Packet Filter" –r "All inbound traffic"
–f *+131.107.1.1 –n BLOCK
```

Die Parameter bedeuten:

- **–w REG –** Schreiben einer statischen Richtlinie in die Registrierung. Dies entspricht exakt der Verwendung der MMC.
- **–p "Packet Filter" –** Hinzufügen zu der vorhandenen Richtlinie namens "Packet Filter".
- **–r "All inbound traffic" –** Erstellen einer Regel namens "All inbound traffic."
- **-f *+131.107.1.1 –** Hinzufügen eines Filters, in dem die Elemente **`*`** eine beliebige Quelladresse und einen beliebigen Port und **`131.107.1.1`** die Zieladresse und einen beliebigen Port festlegen, das Fehlen einer Protokollangabe ein beliebiges Protokoll bedeutet und das Element **+** angibt, dass der Filter gespiegelt wird.
- **–n BLOCK –** Blockieren des Datenverkehrs.

Der letzte Befehl weist die Richtlinie zu:

```
ipsecpol –w REG –p "Packet Filter" –x
```

Die Parameter bedeuten:

- **–w REG –** Schreiben einer statischen Richtlinie in die Registrierung. Dies entspricht exakt der Verwendung der MMC.
- **–p "Packet Filter" –** Hinzufügen zu der vorhandenen Richtlinie namens "Packet Filter".
- **–x –** Zuweisen der Richtlinie.

Mit diesen drei Befehlen haben Sie die gleichen Aufgaben erledigt wie mit der grafischen Benutzeroberfläche. Denken Sie beim Hinzufügen der **IPSECPOL.EXE**-Unterstützung zu Ihren Servereinrichtungsskripts daran, dass Sie die Richtlinie vermutlich erst zuweisen werden, nachdem Sie den Server komplett eingerichtet haben. Deshalb sollte das Skript nur die Befehle **`–n PASS`** und **`–n BLOCK`** enthalten. Nach der Installation aller Server können Sie die Richtlinien unter Verwendung des folgenden Befehls über ein Netzwerk zuweisen:

```
ipsecpol \\machinename –w REG –p "policyname" –x
```

Für den im Befehl angegebenen Computer benötigen Sie Administratorrechte. Wenn Sie die Zuweisung einer Richtlinie vorübergehend aufheben müssen, ersetzen Sie **`–x`** durch **`–y`**.

Sie können eine ganze Richtlinie - einschließlich aller zugeordneten Filterlisten und Filteraktionen - mit folgendem Befehl löschen:

```
ipsecpol –w REG –p "policyname" –o
```

Dies ist zweckmäßig, wenn Sie die Rolle eines Servers während des Servereinrichtungsprozesses dynamisch ändern können, ohne dass ein Neustart erforderlich ist. Löschen Sie die vorhandene Richtlinie, erstellen Sie dann die neue Richtlinie, und weisen Sie diese zu. Sie können **`\\machinename`** zu allen Formen des Befehls hinzufügen, wenn Sie die skriptgesteuerte Erstellung der Richtlinien auf allen Servern über ein Netzwerk durchführen möchten.

***Unterschiede zwischen der grafischen Benutzeroberfläche und "IPSECPOL.EXE".*** Tatsächlich gibt es nur einige wenige Unterschiede hinsichtlich der Art, wie bestimmte Elemente in der grafischen Benutzeroberfläche angezeigt werden.

- Sie können die Standardantwortregel nicht deaktivieren. Dies ist im Falle eines Paketfilters jedoch belanglos, da eingehende Verbindungen immer entweder zugelassen oder blockiert werden.
- Der Name der Regel wird als Name für die Filterliste verwendet.
- Die Befehle **`–n PASS`** und **`–n BLOCK`** verwenden nicht die vorhandenen **Zulassen**- und **Sperren**-Aktionen (wenn letztere auf der grafischen Benutzeroberfläche erstellt wurde). Stattdessen wird für jede Regel eine neue **Zulassen**- bzw. **Sperren**-Aktion erstellt, die den Namen "*Regellistenname* negpol" erhält.
- In den Eigenschaften jeder Filteraktion ist die Standardliste von Sicherheitsmethoden enthalten. Da jedoch keine Sicherheitsaushandlung erfolgt, wird diese Liste ignoriert.
- Beim Löschen einer Richtlinie mit dem Befehl **`–o`** werden auch die zugeordneten Filterlisten und Filteraktionen gelöscht. Dagegen bleiben beim Löschen einer Richtlinie auf der grafischen Benutzeroberfläche die zugeordneten Filterlisten und Filteraktionen erhalten.

# Und das soll tatsächlich funktionieren?

In einem Wort, ja. Kurz nach der Einführung von Windows 2000 testete eine bekannte US-Fachzeitschrift die Sicherheit verschiedener Webserver. Microsoft wurde eingeladen, an diesem Test teilzunehmen. Daraufhin wurde ein Windows 2000-Server mit aktiviertem Internet-Informationsdienste 5.0 eingerichtet. Zur Sicherung des Servers wurde lediglich ein Kennwort zum Administratorkonto hinzugefügt und eine IPSec-Richtlinie wie die in den vorhergehenden Abschnitten erläuterte Richtlinie erstellt. Der Server wurde direkt mit dem Internet verbunden und überstand mehrere Wochen versuchter Angriffe.

Dieser Test wurde allerdings vor dem Entdecken der aktuellen Schwachstellen von IIS 5.0 durchgeführt. Folglich schützt das hier beschriebene Verfahren Ihre Server nicht vor Angriffen über zugelassene Protokolle und Ports. Besuchen Sie deshalb die Website http://www.microsoft.com/technet/security/current.asp (englischsprachig), und installieren Sie die entsprechenden Hotfixes für Ihre Umgebung.

Kommentare oder Fragen zu diesem Artikel sind stets willkommen. Senden Sie Ihr Feedback an technet@microsoft.com (englischsprachig).

[1] Eine *Sicherheitszuordnung* beschreibt die ausgehandelte sichere Kommunikation zwischen zwei Knoten. Sie legt den Authentifizierungstyp, den Verschlüsselungsalgorithmus, das IPSec-Protokoll und die Zieladresse fest.