

FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

**Sicher im Netz: Erfahrungen mit @Guard,
einem persönlichen Firewall für
Window-PCs**

Jürgen Meißburger

FZJ-ZAM-IB-9916

November 1999

(letzte Änderung: 18.11.99)

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | EINLEITUNG..... | 7 |
| 2 | BESCHAFFUNG UND INSTALLATION | 8 |
| 2.1 | AUTOMATISIERTE SOFTWAREBESCHAFFUNG „ONLINE“ | 8 |
| 2.2 | DISTRIBUTION INNERHALB DES FORSCHUNGSZENTRUMS | 8 |
| 2.3 | INSTALLATIONSVORAUSSETZUNGEN..... | 9 |
| 2.4 | DIE INSTALLATION | 9 |
| 2.4.1 | Bei Download vom Server <i>www.atguard.com</i> | 9 |
| 2.4.2 | Bei Download vom Server <i>\\zelcds\</i> | 10 |
| 3 | FUNKTIONALITÄT UND BEDIENUNG..... | 11 |
| 3.1 | DAS MENÜ „SETTINGS“ | 11 |
| 3.2 | DAS „DASHBOARD“ ALS ZENTRALES STEUERELEMENT | 12 |
| 3.2.1 | <i>Eigenschaften des Dashboards</i> | 12 |
| 3.2.2 | <i>Die Anzeige der aktiven Verbindungen</i> | 13 |
| 4 | PROGRAMMEIGENSCHAFTEN UND FILTERKONFIGURATION..... | 14 |
| 4.1 | DIE STARTEIGENSCHAFTEN IM MENÜ „OPTIONS“ | 14 |
| 4.2 | EINRICHTEN VON WEBFILTERN IM MENÜ „WEB“ | 15 |
| 4.2.1 | <i>Das Domänenkonzept</i> | 15 |
| 4.2.2 | <i>Sperren von Werbeinhalten: „Ad Blocking“</i> | 16 |
| 4.2.3 | <i>Die Weitergabe lokaler Benutzerinformationen: „Privacy“</i> | 18 |
| 4.2.4 | <i>Die lokale Ausführung von Programmen: „Active Content“</i> | 19 |
| 4.2.5 | <i>Globale Webfilter-Optionen: „Filters...“</i> | 21 |
| 4.3 | DER FIREWALL UND DIE REGELERSTELLUNG..... | 23 |
| 4.3.1 | <i>Die Funktionsweise des Firewalls</i> | 23 |
| 4.3.2 | <i>Die manuelle Erstellung von Regeln</i> | 24 |
| 4.3.3 | <i>Die halbautomatische Regelerstellung mit dem Regelasistenten</i> | 28 |
| 4.3.4 | <i>Testen einer Regel</i> | 31 |
| 5 | EVENT-LOG UND STATISTIK | 31 |
| 5.1 | DAS EVENT-LOG..... | 31 |
| 5.2 | DIE VERBINDUNGSSTATISTIK | 33 |
| 6 | DER PRAKTISCHE EINSATZ ALS FIREWALL IM JUNET..... | 34 |
| 6.1 | GRUNDSÄTZLICHES ZUR PC-SICHERHEIT | 34 |
| 6.2 | DER „OFFENE PC“ MIT MINIMALEM SCHUTZ | 36 |
| 6.3 | DER „INTRANET-PC“ FÜR DIE FREIE KOMMUNIKATION IM JUNET..... | 37 |
| 6.4 | DER „NORMAL-PC“ MIT NUTZUNGSSPEZIFISCHER KONFIGURATION | 38 |
| 6.5 | DER „SPEZIAL-PC“ MIT MINIMALEM KOMMUNIKATIONSBEDARF..... | 43 |
| 6.6 | DER „GESCHLOSSENE PC“ OHNE AUßENKOMMUNIKATION..... | 43 |
| 7 | AUSBlick | 44 |
| 8 | ANHANG: ATGUARD-INTERNE PORT- UND SERVICENAMEN | 47 |

Verzeichnis der Abbildungen

| | |
|--|----|
| Abbildung 1: Die Programmgruppe „AtGuard“ | 10 |
| Abbildung 2: Das Dashboard | 12 |
| Abbildung 3: Anzeige der aktiven IP-Verbindungen..... | 13 |
| Abbildung 4: Die Startoptionen von AtGuard | 14 |
| Abbildung 5: Das Menü zur Einrichtung der Webfilter..... | 15 |
| Abbildung 6: Darstellung einer Homepage mit GIF-Filter | 17 |
| Abbildung 7: Darstellung der gleichen Homepage ohne Filter..... | 17 |
| Abbildung 8: Kopieren eines Webobjektes..... | 17 |
| Abbildung 9: Zuordnung zur Filterdomäne | 18 |
| Abbildung 10: Der automatisch erstellte Filtereintrag | 18 |
| Abbildung 11: Default-Einstellungen für Privacy..... | 19 |
| Abbildung 12: Empfohlene Einstellungen für „Active Content“ | 21 |
| Abbildung 13: Globale Webfilter-Optionen | 21 |
| Abbildung 14: Der Assistent für Java/ActiveX..... | 22 |
| Abbildung 15: Die Default-Konfiguration des Firewalls..... | 24 |
| Abbildung 16: Erstellen einer neuen Regel von Hand..... | 25 |
| Abbildung 17: Festlegen einer bestimmten Applikation..... | 26 |
| Abbildung 18: Die Definition der Serviceports | 26 |
| Abbildung 19: Spezifikation einer Netzwerkadresse | 27 |
| Abbildung 20: Einstellen der Gültigkeitszeiten einer Regel..... | 28 |
| Abbildung 21: Loggen einer Regel | 28 |
| Abbildung 22: Ein FTP-Verbindungsversuch im Fenster des Regelassistenten..... | 29 |
| Abbildung 23: Der Eintrag im Eventlog durch den Regelassistenten..... | 29 |
| Abbildung 24: Bestätigung der Applikation | 29 |
| Abbildung 25: Bestätigung des Service-Ports (FTP-Kontrollverbindung) | 30 |
| Abbildung 26: Quelladresse der Verbindungsanforderung..... | 30 |
| Abbildung 27: Die mit dem Regelassistenten erstellte neue Regel | 30 |
| Abbildung 28: Test einer Firewall-Regel..... | 31 |
| Abbildung 29: Das Event-Log mit der Anzeige der IP-Verbindungen..... | 32 |
| Abbildung 30: Anzeige der gesperrten Webinhalte | 32 |
| Abbildung 31: Die Anzeige aktivierter Regeln des Firewalls..... | 33 |
| Abbildung 32: Loggen von Privacy-Ereignissen | 33 |
| Abbildung 33: Die Anzeige der Web- und Verbindungsstatistik | 34 |
| Abbildung 34: Die Regeln für freie Kommunikation im Intranet..... | 38 |
| Abbildung 35: Regeln eines anwendungsspezifisch gesicherten „Normal-PCs“ | 42 |

Verzeichnis der Tabellen

| | |
|---|----|
| Tabelle 1: Regeln für die offene Kommunikation | 36 |
| Tabelle 2: Regeln für die freie Kommunikation im JuNet..... | 37 |
| Tabelle 3: Logging von NETBIOS-Zugriffen..... | 38 |
| Tabelle 4: Eine Einzelregel zum Sperren eines Teilnetzes | 38 |
| Tabelle 5: Individuelle Konfiguration eines typischen JuNet-PCs | 39 |
| Tabelle 6: Der Spezial-PC mit minimalem Kommunikationsbedarf | 43 |
| Tabelle 7: Der PC ohne Außenkommunikation | 44 |

1 Einleitung

Wer hat nicht schon einmal vor seinem ans Internet angeschlossenen PC gesessen und sich gewundert, wenn dieser plötzlich und ohne eigenes Zutun unüberhörbare Eigenaktivität zu entwickeln scheint: Das vertraute Geräusch der zum Leben erwachten Festplatte und die nervös blinkenden LEDs an der Vorderseite beunruhigen doch ein wenig, und man möchte in diesem Augenblick nur zu gerne wissen, was der PC „da eigentlich tut“ oder gar „wer auf dem PC da etwas zu tun hat“! Ähnlich beunruhigend mag eine Meldung sein, die man gelegentlich beim Herunterfahren des Systems lesen kann, ohne daß man sich vielleicht der Ursache dieser Meldung bewußt wäre: „Es sind noch 1 Benutzer mit Ihrem System verbunden“. Täglich erfährt man in den Medien, daß Scharen hoch qualifizierter und motivierter „Hacker“ sich rund um die Uhr damit vergnügen, in die Systeme ihrer ahnungslosen Internet-Mitstreiter einzudringen, um höchst persönliche oder gar geheime Daten auszuspionieren, diese Daten zu manipulieren, mit Computerviren zu infizieren oder einfach zu zerstören. Sicherheit im Internet ist *das* große Thema – und nicht ohne Grund, exponiert man sich mit seinem System doch einer weltweiten Gemeinschaft von mehr als 50 Millionen Internetnutzern.

Tatsache ist, daß alle Netzwerk-Betriebssysteme – und Windows macht da ebensowenig wie Unix eine Ausnahme – eine solch hohe Komplexität aufweisen, daß sich immer wieder Fehler und Schwachstellen in die Softwareimplementierung einschleichen, die von Kennern der Betriebssystem-Interna für ihre Angriffe mißbraucht werden können. Wer nur eine FAQ-Liste zum Thema Sicherheits-Patches im Internet liest, gewinnt rasch den Eindruck, daß es schier unmöglich scheint, das Betriebssystem selbst gegen alle Angriffsversuche aus dem Netz abzusichern. Eine weitere, vielleicht sogar die häufigste Fehlerquelle liegt in der menschlichen Unzulänglichkeit der Benutzer selbst, die aus Bequemlichkeit, Vergeßlichkeit oder einfach aus Unkenntnis bekannte Sicherheitslücken nicht schließen oder durch unbedachte Nutzung der gegebenen Möglichkeiten selbst solche erst auf tun.

Aus diesen Erfahrungen heraus sind Sicherheitskonzepte für Rechner in solch großen Netzen wie eben dem Internet heute im allgemeinen mehrschichtig angelegt: Man versucht, die Sicherheit der angeschlossenen Systeme selbst so gut wie eben möglich und ohne große Einbußen an Arbeitsqualität zu gewährleisten, gleichzeitig aber erhöht man die Sicherheit des eigenen Netzes durch den Einsatz von Firewall-Lösungen an der Schnittstelle zur Außenwelt. Dies sind leistungsfähige und nicht eben billige Spezialsysteme, die den Verbindungsaufbau und den Datenverkehr von außen ins eigene Netz authentisieren, filtern und dokumentieren und im Extremfall vollkommen verschlüsseln. Hierzu sind komplexe Rechenvorgänge erforderlich, die bei der Leistungsfähigkeit heutiger Netze im allgemeinen nicht ohne Verlust an Übertragungsgeschwindigkeit zu realisieren sind. Aus diesen Gründen wird häufig zugunsten der Leistungsfähigkeit der Netze auf den zentralen Einsatz solcher Firewalls verzichtet.

Hier nun kommt eine dritte Möglichkeit zum Tragen, die Gegenstand des folgenden Erfahrungsberichtes ist: Die Einrichtung eines Firewalls auf dem betroffenen Endsystem selbst, mit dem die gesamte Kommunikation von und zu den Netzen beobachtet, gefiltert und gegebenenfalls verhindert werden kann. Diese Lösung hat nebenbei den Vorteil, daß sie auch gegen Attacken aus dem eigenen, firmen- oder hausinternen Netz greift, sollte dort einmal ein Rechner von einem „Hacker“ übernommen und für Angriffsversuche „von innen“ mißbraucht werden. Des weiteren bietet sie gegenüber einem zentral verwalteten Firewall den Vorteil, daß sich der Benutzer ein genau auf seine Wünsche zugeschnittenes Sicherheitsprofil einrichten und dieses auch jederzeit selbst ändern kann.

Das Prinzip eines solchen Firewalls besteht darin, daß alle ein- und auslaufenden IP-Pakete nach Herkunft- und Zieladresse und nach dem IP-Port analysiert werden, der die Art des

Dienstes („**service**“) wie beispielsweise „Telnet“ für interaktive Verbindungen oder „FTP“ für den Dateitransfer charakterisiert. Für jeden denkbaren Typ einer solchen Verbindung können Regeln erstellt werden, die weitere Kriterien wie z.B. Art der Anwendung oder die Tageszeit berücksichtigen und als Ergebnis den Verbindungsaufbau zulassen oder ablehnen. Die Verbindungsdaten selbst und die Ergebnisse der Regelauswertung können in einem Log erfaßt und statistisch ausgewertet werden.

Die hier vorgestellte Software „**AtGuard**“ oder „**@Guard**“ ist ein solcher regelbasierter Firewall für Internet-PCs, die den Microsoft-eigenen IP-Stack benutzen. Zusätzlich erfüllt AtGuard die Funktion eines Webfilters, das unabhängig und ergänzend zu den im Browser selbst möglichen Sicherheitseinstellungen das Filtern bestimmter lästiger oder auch potentiell gefährlicher Webinhalte erlaubt.

Die vielleicht interessanteste Funktion von AtGuard ist der sogenannte Regelassistent („**RuleAssistant**“). Er wird automatisch aktiviert, wenn ein „neuer“, d.h. durch keine bisher definierte Regel erfaßter Kommunikationstyp erkannt wird, und unterstützt menügeführt die Erstellung einer entsprechenden neuen Regel. Dieser Regelassistent ist ein hervorragendes Hilfsmittel, um das eigene Kommunikationsumfeld besser kennen und verstehen zu lernen, und mit seiner Hilfe können beispielsweise Scan-Versuche von außerhalb oder nicht erwünschte und häufig überflüssige Kontaktversuche von fehlkonfigurierten Maschinen im eigenen Netz sehr leicht erkannt und identifiziert werden.

2 Beschaffung und Installation

2.1 Automatisierte Softwarebeschaffung „online“

Das diesem Bericht zugrunde liegende Produkt ist lauffähig unter Windows 95, 98 und NT. Der Anbieter der Software (<http://www.atguard.com>), die Fa. WRQ, hat die gesamte Vertriebsabwicklung an den E-Commerce-Anbieter www.netsales.net delegiert, der Lizenzen und Software-Kits ausschließlich online über Webformulare und Download anbietet. Ein Kauf der Software auf Datenträger bei einem der lokalen Büros von WRQ ist derzeit nicht möglich! Die Zahlung kann per Kreditkarte, Orderscheck (US-Dollar) oder internationale Banküberweisung erfolgen. Die für die letztgenannten Zahlungsmodalitäten erforderlichen Daten wie Firmenadresse oder Kontoinhaber sind jedoch ebenfalls erst **nach** Ausfüllen einer Online-Bestellung über das Webinterface zugänglich. Dieser Ansatz eines „reinen“ Online-Marketing ist sicher zum schnellen Kauf einer Einzellizenz per Kreditkarte für Anbieter wie Käufer recht bequem, für größere Firmen mit einer noch überwiegend an die Papierform gebundenen Verwaltung jedoch kaum handhabbar.

Mit dem Kauf einer Lizenz erhält man per Email eine (automatisch generierte) elektronische Kaufbestätigung, eine Bestellnummer und einen digitalen Schlüssel, mit dessen Hilfe man den gepackten Softwarekit nach dem Herunterladen vom Server entpacken kann

2.2 Distribution innerhalb des Forschungszentrums

Für das Forschungszentrum Jülich hat das ZAM inzwischen eine begrenzte Zahl von Lizenzen erworben, so daß die Software auf dem FZJ-internen Distributionsserver `\\zelcds\` unter dem Share

`\\zelcds\atguard`

zum Herunterladen bereitgestellt werden kann. Zugriffsberechtigung besitzen die PC-Verantwortlichen der Organisationseinheiten, die auf Grund ihrer Kenntnisse der IP-

Infrastruktur von JuNet die Installation und Konfiguration vor Ort betreuen und bei der Erstellung geeigneter Firewallregeln für die betreuten Endsysteme behilflich sein können. Ergänzt wird das Angebot durch eine Kurzfassung der Installationsanleitung unter

\\pcsrv\atguard\readme.txt

und eine technische Kurzinformation ZAM-TKI-0349 unter

http://www.fz-juelich.de/zam/docs/tki/tki_html/t0349/t0349.html ,

die die grundsätzlichen Funktionen der Software und ihrer Anwendung anhand eines einfachen Beispiels kurz umreißt.

2.3 Installationsvoraussetzungen

Die Software ist lauffähig auf Microsofts Windows-Betriebssystemen Windows 95, 98 und NT 4.0. Sie benötigt keine besondere Hardware oder Treiber, sondern setzt vollständig auf den Betriebssystemstandards von Microsoft auf. Sie ist damit auf jedem „normalen“ PC, der den Microsoft IP-Stack benutzt, also z.B. auch auf Laptops, lauffähig. Sie wurde auf einem Laptop mit Pentium I/90 unter Windows 95, einem Pentium I/166 unter Windows 98 sowie Pentium II/266 und Pentium III/500-Rechnern unter Windows NT 4.0 Workstation erfolgreich getestet und eingesetzt.

Die vom Server des Herstellers heruntergeladene Datei „**atg.exe**“ ist ein selbstentpackendes Archiv, das durch Ausführen in einem beliebigen, temporären Verzeichnis den eigentlichen Installationskit , z.B. „**atgd310.exe**“ für die Version 3.10 erstellt. Hierzu wird zwingend die Lizenzinformation benötigt, die man zuvor vom E-Commerce-Server per Email erhalten hat. Eine Kopie des so erhaltenen, lizenzierten Installationskits sollte für eine später eventuell notwendige Nachinstallation auf jeden Fall an einem sicheren Platz aufbewahrt werden.

Die Softwareinstallation benutzt wie üblich den Microsoft Install-Shield und ist damit problemlos durch Ausführen von „atgd310.exe“ im System zu installieren und auch wieder mit Hilfe der Systemsteuerung oder des Uninstall-Links in der AtGuard-Programmgruppe zu entfernen. Alle Softwarekomponenten werden korrekt in einem eigenen Ordner je nach Nationalitäteneinstellung des Systems unter „C:\Programme“ bzw. „C:\Programs“ installiert und benötigen ca. 2,2 MB auf der Festplatte.

Auf dem Campus-Server \\zelcds\atguard liegen die bereits entpackten, lizenzierten Installationskits und deren Updates, die direkt und ohne nochmalige Angabe einer Lizenznummer installiert werden können.

2.4 Die Installation

2.4.1 Bei Download vom Server www.atguard.com

Der heruntergeladene "unpacking wizard" **atg.exe** wird auf ein temporäres Verzeichnis, z.B. C:\Temp kopiert und dort durch Doppelklick ausgeführt:

```
Ausführen c:\Temp\atg.exe (unpacking wizard)
Next
Serial # ..... Eingabe der Seriennummer
Digital Key ..... Eingabe der Schlüsselinformation
Next
C:\Temp als temporäres Verzeichnis angeben
Next - Next – Finish
```

Damit wird der eigentliche Installationskit (**atgd310.exe**) nach C:\Temp entpackt und der AtGuard Setup Installation Wizard automatisch gestartet.

2.4.2 Bei Download vom Server \\zelcds\

Die Installation wird direkt durch Ausführen von **atgd310.exe** gestartet. Nach Abschluß der Installation

... Installation von AtGuard V3.1
Next - Yes
Installationspfad C:\Programme\Atguard
Next
Program Folders: AtGuard
Next – Next

Yes, I want to restart my computer now:

Falls weitere Updates vorliegen, können diese in gleicher Weise nacheinander installiert werden, und der Reboot wird nach Einspielen des letzten Updates mit

Yes, I want to restart my computer now: Finish

durchgeführt.

Nach dem Reboot steht AtGuard als Applikation mit einer eigenen Programmgruppe „AtGuard“ zur Verfügung. Die Links der neuen Gruppe werden unter Windows NT im Benutzerprofil „All Users“ abgelegt, so daß sie allen Benutzern des Systems zur Verfügung stehen:

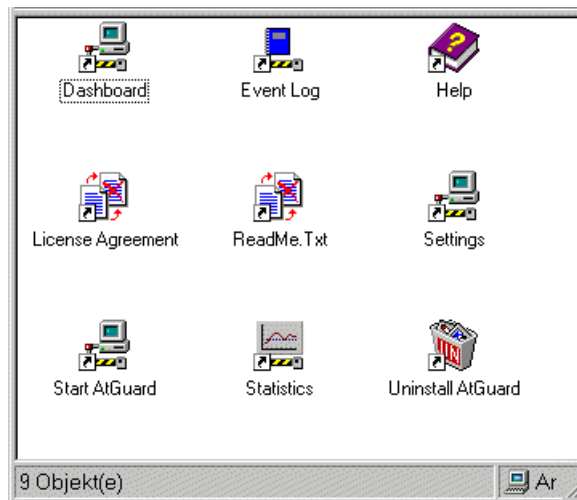




Abbildung 1: Die Programmgruppe „AtGuard“

Die verschiedenen Programmfunktionen sind im einzelnen:

- **Dashboard:** Ein zentrales Bedienelement für die Firewallfunktionen ähnlich der Taskleiste von Windows. Hier können einzelne Filterfunktionen oder auch das ganze Firewallsystem bequem ein- und ausgeschaltet werden.
- **Event Log:** Hier werden alle Netzwerk-relevanten Ereignisse wie Verbindungsaufbau oder das Ansprechen von Auswahlregeln des Firewalls notiert.
- **Settings:** Damit werden die Starteigenschaften von AtGuard, seine Webfilter und Firewallregeln konfiguriert. Dieses Programm *muß* zu Beginn einmal durchlaufen werden.

- **Start AtGuard:** Startet die Software im Hintergrund mit einem Icon  im SystemTray.
- **Statistics:** Zeigt in Gruppen geordnet eine Langzeitstatistik der IP-Verbindungen.
- **License Agreement:** Der Text der Lizenzvereinbarungen.
- **ReadMe.Txt:** Installations-, Konfigurations- und Versionshinweise.
- **Help:** Windows-Hilfdatei mit Bedienungsanleitung.

Diese Programme können durch Doppelklick auf das entsprechende Symbol der Programmgruppe oder durch Klick auf das Popup-Menü des weiter unten beschriebenen „Dashboards“ aktiviert werden. Einfacher und bequemer ist jedoch ein Klick auf das Symbol  im SystemTray, wo alle Funktionen in einem Popup-Menü angeboten werden. Hier können auch mit „Disable“ alle Funktionen von AtGuard mit einem Mausklick deaktiviert werden, ohne die übrigen Einstellungen permanent zu verändern.

3 Funktionalität und Bedienung

AtGuard bietet zwei grundsätzliche Funktionalitäten: Zum einen die Funktion eines

Webfilters,

mit dessen Hilfe Webinhalte vor deren Interpretation durch den Browser gefiltert werden. Diese Funktion ergänzt damit die Sicherheitseinstellungen des Webbrowsers um eine äußere, von den Einstellungen des Webbrowsers unabhängige Sicherheitsschale.

Zum andern bietet AtGuard die Funktion eines

Internet-Firewalls,

mit dem ein- und auslaufende IP-Pakete analysiert und der Verbindungsaufbau regelbasiert erlaubt oder verhindert werden kann. Diese beiden Funktionen sind unabhängig voneinander nutzbar und können wahlweise an- oder abgeschaltet werden.

3.1 Das Menü „Settings“

Alle Einstellungen, insbesondere die Einstellungen der Webfilter- und Firewallfunktionen und die Definition der Firewallregeln werden über das Konfigurationsmenü "**Settings...**" vorgenommen. Beim ersten Aufruf von AtGuard wird der Benutzer, falls er dies nicht ohnehin schon zu Beginn getan hat, aufgefordert, das Menü „Settings“ zu durchlaufen, um die grundsätzlichen Einstellungen festzulegen. Das Menü hat drei Unterpunkte, die weiter unten im Detail besprochen werden:

- **Options** zur Einstellung der Laufeigenschaften des Programms selbst,
- **Web** zur Definition der Filter für das Webbrowsing und
- **Firewall** zur Definition des Verhaltens des IP-Firewalls (Regeldefinition).

Ergänzend zu diesen eigentlichen Grundfunktionen des Programms werden einige Hilfsfunktionen angeboten, die den praktischen Betrieb bequemer gestalten wie z.B. das Steuerelement „**Dashboard**“ sowie **Logging-** und **Statistikfunktionen**, die einen recht guten Überblick über die gesamte Kommunikation des PCs im Internet gewähren.

Besonders interessant ist auch die unmittelbare Anzeige der aktuell von und zu dem PC bestehenden Internetverbindungen, aus denen ersichtlich ist, welche Dienste der PC selbst im Internet anbietet („**local service**“) bzw. zu welchen lokalen Diensten Verbindungen aus dem

Internet versucht werden („**inbound**“). In der umgekehrten Richtung („**outbound**“) wird erfaßt, zu welchen externen Diensten der PC eine Internetverbindung aufzubauen versucht oder aufrecht erhält („**remote service**“).

3.2 Das „Dashboard“ als zentrales Steuerelement

3.2.1 Eigenschaften des Dashboards

Das zentrale Anzeige- und Steuerelement für AtGuard im laufenden Betrieb ist das **Dashboard**,



Abbildung 2: Das Dashboard

in dem durch Anklicken der **Auswahlkästchen** die Funktionen


- AtGuard (Webfilter und Firewall) insgesamt,
- „Ads Blocking“ (Blockieren von Werbeinhalten in Webseiten),
- „Privacy Protection“ (Cookies und Weitergabe von Benutzerinformation)
- und „Firewall Activity“ (IP-Firewall)

unmittelbar ein- bzw. ausgeschaltet werden können. Das Dashboard selbst läßt sich sinnvollerweise nur aktivieren, wenn AtGuard aktiviert ist. Versucht man es dennoch, ohne daß AtGuard vorher gestartet wurde, so erhält man eine Fehlermeldung mit der Aufforderung, AtGuard zu starten.

Daneben werden im Dashboard **Summenzähler** für bestimmte Typen von Verbindungen oder Ereignissen angezeigt:

- Zahl der aktiven Netzverbindungen („sockets“)
- Zahl der aktiven Webverbindungen
- Zahl der abgeblockten Web-Werbeinhalte
- Zahl der abgeblockten Cookies und Referer-Informationen
- Zahl der vom Firewall erlaubten und abgelehnten IP-Verbindungen

Das Dashboard läßt sich im typischen Windows-Stil wie eine Taskleiste am oberen Bildrand „docken“, oder es läßt sich als frei bewegliches Fenster irgendwo auf dem Bildschirm ablegen. Für die Praxis ist die gedockte Position in allen Fällen vorzuziehen.

Auf der linken Seite des Dashboard befindet sich das Symbol . Durch einen Mausklick auf dieses Symbol klappt ein Menü auf, in dem verschiedene Einstellungen zum Dashboard selbst vorgenommen und auch die bereits besprochenen Hilfsprogramme gestartet werden können.

Sollte das Dashboard gelegentlich stören, so kann es mit „**Hide Dashboard**“ im Menü gänzlich abgeschaltet und jederzeit durch einen Mausklick auf das Symbol im SystemTray mit „**Dashboard**“ wieder eingeschaltet werden. Beim Aktivieren des Dashboards werden übrigens die Fenster anderer Applikationen, die in den Raum des Dashboard hineinragen und von diesem teilweise überdeckt werden würden, automatisch auf die passende Größe reduziert.

In dem Untermenü „**Properties**“ des Dashboards lassen sich weitere Einstellungen zum Erscheinungsbild vornehmen: Mit „**Always on Top**“ bleibt das Dashboard ständig sichtbar, mit

„**Autohide**“ verschwindet das Dashboard ähnlich der Windows-Taskleiste, sobald die Maus aus seinem Fenster hinausbewegt wird. In diesem Untermenü kann auch ausgewählt werden, welche Funktionen in diesem Dashboard mit ihren Zählern angezeigt werden sollen. Wer beispielsweise nur Webfilter, aber keinen Firewall benötigt, kann die betreffende Anzeige hier auch ausschalten. Wohl bemerkt schaltet man hier nur die Anzeige der Firewallaktivität ab, nicht jedoch die Funktion des Firewalls selbst! Dies läßt sich leicht über das Untermenü „Settings“ nachprüfen. Das Dashboard zeigt mit den angezeigten Zählern die aktuelle Summenstatistik zu IP-Verbindungen, Webaktivität, Webfiltern und Firewall-Filtern.

Ganz rechts im Dashboard befindet sich noch das Icon eines Mülleimers, der dazu benutzt werden kann, unerwünschte Elemente und Links aus einer gerade im Browser betrachteten Webseite auf sehr bequeme Art und Weise mit „copy & paste“ in die Liste der zu sperrenden Webinhalte aufzunehmen. Dies wird weiter unten im Absatz „Webfilter automatisch erstellen“, in Kapitel 4.2 genauer beschrieben.

3.2.2 Die Anzeige der aktiven Verbindungen

Eine der nützlichsten Funktionen des Dashboards ist die momentane Anzeige aller bestehenden IP-Verbindungen: Ein Mausklick auf die Zahl der offenen Netzwerkverbindungen (in unserem Beispiel 15) zeigt eine Liste der gerade aktiven Verbindungen mit Protokollinformation, Adressen, Status und Paketstatistik:

| Proto | Executable | State | Remote | Local | Sent | Received | Time |
|-------|--------------|---------------|-----------------|--------------------|------|----------|---------|
| TCP | inetinfo.exe | Listening | | zam125: http | 0 | 0 | 1:39:49 |
| TCP | inetinfo.exe | Listening | | localhost: 1027 | 0 | 0 | 1:39:53 |
| TCP | inetinfo.exe | Listening | | zam125: 1028 | 0 | 0 | 1:39:52 |
| TCP | RPCSS.EXE | Listening | | zam125: dcom | 0 | 0 | 1:39:54 |
| TCP | RPCSS.EXE | Connected/Out | localhost: 1026 | localhost: 1034 | 9 | 0 | 1:39:33 |
| TCP | RPCSS.EXE | Connected/In | localhost: 1034 | localhost: 1026 | 0 | 9 | 1:39:33 |
| TCP | System | Listening | | zam125: nbssession | 0 | 0 | 1:40:01 |
| TCP | war-ftp.exe | Listening | | zam125: ftp | 0 | 0 | 1:39:44 |
| UDP | explorer.exe | Listening | | localhost: 1047 | 67 | 67 | 1:28:44 |
| UDP | RPCSS.EXE | Listening | | zam125: dcom | 0 | 4080 | 1:39:54 |
| UDP | System | Listening | | zam125: nbname | 476 | 67370 | 1:40:01 |
| UDP | System | Listening | | zam125: nbdatagram | 2427 | 152688 | 1:40:01 |
| UDP | war-ftp.exe | Listening | | zam125: 1033 | 0 | 0 | 1:39:44 |
| UDP | war-ftp.exe | Listening | | zam125: portmap | 0 | 88 | 1:39:44 |


Abbildung 3: Anzeige der aktiven IP-Verbindungen

Der Eintrag „Listening“ bedeutet, daß für diesen IP-Port auf dem lokalen PC ein Server („Dienst“) gestartet ist, der auf Verbindungsanfragen von außen reagiert. Diese aktiven Ports werden von Hackern gerne benutzt, um sich durch Ausnutzen von Fehlern oder Sicherheitslücken in der Softwareimplementierung einen ersten Zugang zu Fremdsystemen zu verschaffen. Es bietet sich daher an, mit Hilfe der Firewallfunktion solche Ports besonders aufmerksam zu überwachen oder deren Benutzung auf bestimmte IP-Adreßbereiche (beispielsweise nur alle Adressen des hausinternen Netzes) oder Tageszeiten (nur zur regulären Arbeitszeit) zu beschränken.

Wo eine Zuordnung einer Portnummer zu einem bekannten Dienst möglich ist, wird wie auch bei der weiter unten beschriebenen Regelbildung für den Firewall der Name des Dienstes an Stelle der Portnummer angezeigt, also beispielsweise **zam125:http** (ein laufender Webserver) statt **zam125:80**. Die Portzuordnung zu den Dienstnamen entnimmt AtGuard einerseits der systemeigenen Tabelle „**services**“ (C:\Windows\services unter Windows 95/98 bzw. C:\Winnt\System32\Drivers\etc\services unter Windows NT), andererseits einer internen Tabelle, die im AtGuard-Help unter „**AtGuard Port And Service Assignments**“ dokumentiert ist (siehe Anhang).

4 Programmeigenschaften und Filterkonfiguration

Das Konfigurationsmenü „Settings“ kann sehr flexibel

- aus der Programmgruppe durch Doppelklick des Icons "Settings",
- durch Klick auf "Settings..." im Pulldown-Menü des Dashboards
- oder durch Klick auf das Symbol  im SystemTray und "Settings..."

aufgerufen werden. Die letztgenannte Möglichkeit ist besonders bequem, weil das Symbol im TaskTray bei sichtbarer Taskleiste ebenfalls stets sichtbar ist.

4.1 Die Starteigenschaften im Menü „Options“

Allgemeine Startoptionen von AtGuard werden in diesem Menü festgelegt:

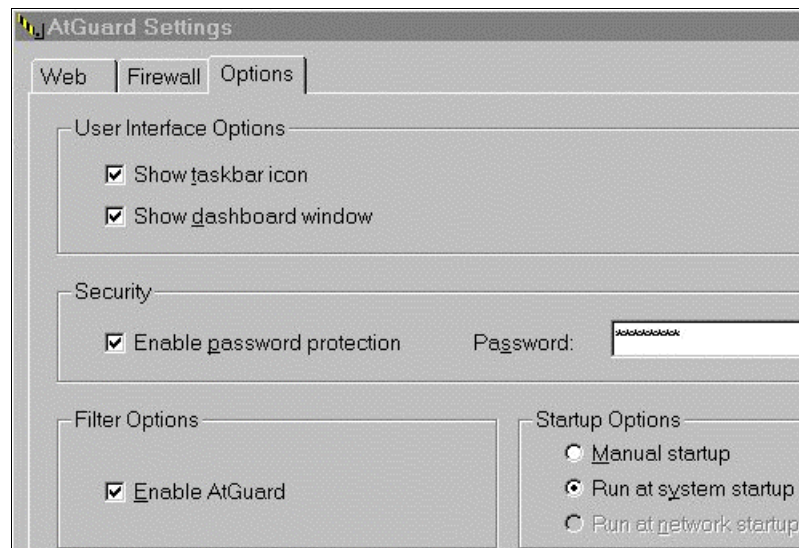



Abbildung 4: Die Startoptionen von AtGuard

In den „**User Interface Options**“ können die Anzeige des Icons im SystemTray und des Dashboards beim Programmstart abgeschaltet werden. Da dann nur der umständliche Weg über die Programmgruppe bleibt, sollten diese unbedingt beim Programmstart eingeschaltet bleiben.

Die „**Security**“-Option ermöglicht den Schutz der Einstellungen, insbesondere der im Firewall aktivierten Filter, durch ein Paßwort. Dies ist für einen stabilen Produktionsbetrieb nach Abschluß einer gewissen Lernphase empfehlenswert, während der man zunächst einmal mit Hilfe des unten beschriebenen Regelassistenten einen Überblick über die eigenen Aktivitäten im Netz gewinnt. Während dieser Lernphase sollte man temporär den Paßwortschutz abschalten, da sonst wiederholt bei jedem neuen Verbindungstyp, für den der Assistent eine Regel erstellt, das Paßwort eingegeben werden muß. (Selbstverständlich wird hier vorausgesetzt, daß der Zugang zum Betriebssystem selbst durch Paßwort und Bildschirmschoner geschützt ist!).

Unter „**Filter Options**“ läßt sich festlegen, ob AtGuard im aktivierten oder deaktivierten Zustand gestartet wird. Der deaktivierte Zustand wird im Dashboard und im TaskTray durch das Symbol  angezeigt. Dieser definierte Anfangszustand wird auch bei einem Neustart des Programms wieder hergestellt, so daß die Steuerungsmöglichkeiten über die Symbole im Dashboard und im TaskTray auch in abgeschaltetem Zustand erhalten bleiben. In abgeschal-

tetem Zustand sind sämtliche Webfilter und die Prüfung der IP-Pakete nach den Regeln des Firewalls außer Kraft gesetzt!

Die Einstellungen in „**Startup Options**“ lassen die Wahl zwischen einem automatischen Start mit dem Hochfahren des Systems oder einem manuellen Start über „**Start AtGuard**“ in der Programmgruppe. Wegen der bequemen Steuermöglichkeiten über den TaskTray und das Dashboard empfiehlt sich sicher der automatische Start mit dem Betriebssystem.

Eine dritte Möglichkeit „**Run at Network Startup**“ ist vor allem für Rechner interessant, die über Modem- oder ISDN-Strecken mit Hilfe der Windows-eigenen DFÜ- oder RAS-Dienste temporäre Internetverbindungen aufbauen. In diesem Fall wird AtGuard automatisch mit dem Start der Netzwerkverbindung aktiviert und bei deren Beenden wieder deaktiviert. Diese Option steht allerdings nur für Windows 95/98, nicht jedoch für Windows NT zur Verfügung. Bei Verwendung des für den Zugang zum ISDN-Server des Forschungszentrums häufig eingesetzten CANDI-ISDN-Treibers, der sich im System wie ein LAN-Treiber verhält, ist dieser Startmechanismus ebenfalls nicht verfügbar.

4.2 Einrichten von Webfiltern im Menü „Web“

In diesem Untermenü von „Settings“ werden alle Einstellungen vorgenommen, die das Verhalten des lokalen Webbrowsers – üblicherweise Internet Explorer oder Netscape – beim „Browsen“ der Inhalte einer Website im Netz betreffen. Das beinhaltet einerseits die Weitergabe lokal existierender Benutzerinformationen (z.B. Mailadressen oder Cookies) an den fremden Webserver, andererseits die gesonderte Behandlung bestimmter Webinhalte wie animierte Grafiken oder Werbeeinlagen.

4.2.1 Das Domänenkonzept

Das Menü zur Einrichtung der Webfilter ist zweigeteilt:

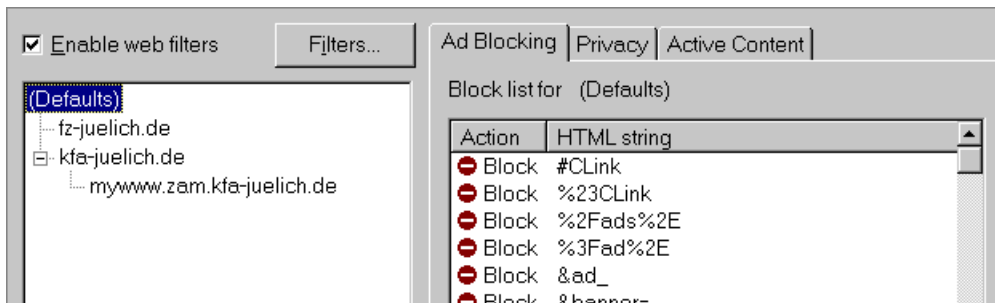


Abbildung 5: Das Menü zur Einrichtung der Webfilter

Auf der linken Seite findet man unterhalb eines Auswahlkästchens zur Aktivierung oder Deaktivierung aller Webfilter (gleiche Funktion wie im Dashboard) eine Baumstruktur von IP-Domänen und Rechnernamen unterhalb einer „Defaults“-Wurzel hierarchisch angeordnet. Im ausgelieferten Zustand kennt AtGuard nur diese Domäne „Defaults“, die mit dem Knopf „Add Site“ nach Belieben durch weitere Domänen oder Rechnernamen erweitert werden kann.

Für jeden einzelnen Eintrag in dieser Domänenliste lassen sich auf der rechten Seite unterschiedliche Einstellungen für „Ad Blocking“, „Privacy“ und „Active Content“ vornehmen und abspeichern. Damit ist man in der Lage, für vertrauenswürdige, beispielsweise in eigener Verantwortung betriebene Webserver oder auch für ganze als vertrauenswürdige eingestufte Domänen spezifische Sätze von Webfiltern einzurichten. Dabei folgt die Gültigkeit der Filterregeln der hierarchischen Struktur des Baumes, indem jede untergeordnete Ebene zunächst

die Eigenschaften der übergeordneten Domäne erbt. Diese vererbten Einstellungen können dann durch entsprechende Modifikationen einzelner Parameter auf der rechten Seite Domänen-spezifisch durch Aktivieren des Kästchens „Use these rules for *Domänenname*“ überschrieben werden. Sind keine speziellen Regeln aktiv, so wird unten im Menü nochmals in roter Schrift ein Hinweis auf die tatsächlich benutzten Regeln der übergeordneten Domäne angezeigt

Für den Betrieb in einem Intranet wie beispielsweise dem JuNet des Forschungszentrums Jülich bietet es sich an, die Default-Einstellungen einigermaßen restriktiv zu halten, während die beiden firmeninternen Domänen „fz-juelich.de“ und „kfa-juelich.de“ bezüglich „Privacy“- und „Active Content“-Einstellungen wesentlich offener behandelt werden können. Die Defaulteinstellungen für „Ad Blocking“, die von der übergeordneten Default-Domäne geerbt werden, treffen hier ohnehin nicht zu und stören deshalb nicht.

4.2.2 Sperren von Werbeinhalten: „Ad Blocking“

4.2.2.1 Webfilter von Hand erstellen

Die Domäne „Default“ wird bereits vom Hersteller mit einer umfangreichen Liste typischer HTML-Muster ausgeliefert, um Inhalte bestimmter Webserver oder einzelne Objekte, die auf Werbeinhalte hindeuten, zu sperren. Die Liste dieser Filter enthält zwei Spalten: Die erste Spalte mit dem Eintrag „permit“ oder „block“ je nach gewünschter Aktion und die zweite Spalte mit einem Textmuster, nach dem AtGuard den Webinhalt durchsucht und im Falle eines „block“ diesen von der Webseite vor deren Anzeige entfernt bzw. im Falle eines „permit“ auf der Webseite beläßt. Die Aktion „permit“ wird benötigt, um Links einer untergeordneten Domäne, die in einer übergeordneten Hierarchiestufe geblockt wurden, zu reaktivieren. Neue HTML-Muster werden mit dem Knopf „Add“ im Untermenü „Ad Blocking“ mit der Aktion „block“ oder „permit“ eingetragen, mit „Modify“ modifiziert und mit „Remove“ wieder gelöscht.

An dieser Stelle sei ausdrücklich darauf hingewiesen, daß die Voreinstellungen in „Ad Blocking“ im wesentlichen auf amerikanische (bzw. englischsprachige) Anbieter zugeschnitten und deshalb innerhalb Deutschlands nur begrenzt wirksam sind. Dies ist neben dem Fehlen einer deutschsprachigen Version von AtGuard wohl auch einer der Gründe, weshalb AtGuard vom Hersteller selbst in Deutschland nicht vertrieben wird. Wer in diesem Sprachraum Werbeinhalte wirksam unterdrücken möchte, muß entsprechende deutschsprachige Wortmuster selbst der Filterliste entweder von Hand oder mit Hilfe des im nächsten Abschnitt beschriebenen Trashcan-Mechanismus hinzufügen.

Als Muster eines zu sperrenden Webinhalts können beliebige Zeichenkettenausdrücke benutzt werden, die Bestandteil eines URL sein können. Mit

block microsoft.com

würden beispielsweise alle Webinhalte der Domäne microsoft.com ausgeblendet, mit

block .gif in der Domäne fz-juelich.de

würden alle GIF-Bilder auf der Homepage und auf sämtlichen Webseiten aller Server in der Domäne fz-juelich.de des Forschungszentrums Jülich ausgeblendet. Die Fußzeile dieser Homepage sähe dann wie folgt aus,

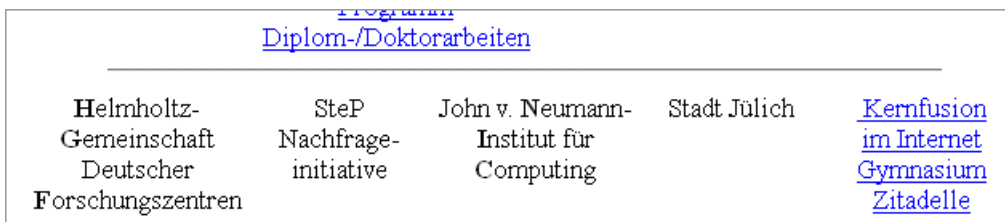


Abbildung 6: Darstellung einer Homepage mit GIF-Filter

während die gleiche Homepage, adressiert über die Domäne „kfa-juelich.de“ anstatt über „fz-juelich.de“ ein ganz anderes Bild liefert:

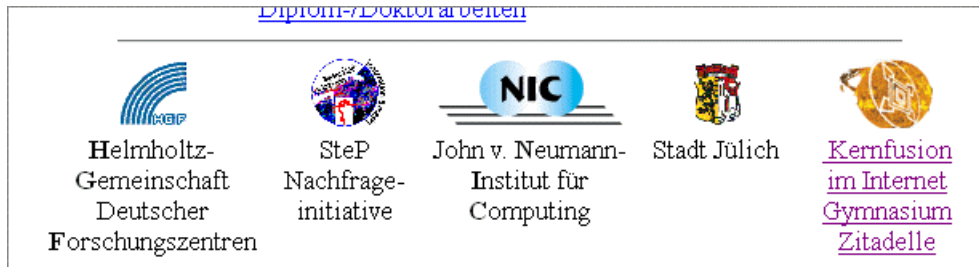


Abbildung 7: Darstellung der gleichen Homepage ohne Filter

Diese derzeit noch beim Server des Forschungszentrums mögliche, aber auch im Internet häufig zu findende Doppeladressierung eines Webservers ist im übrigen eine ideale Möglichkeit, solche domänenspezifischen Filtereinstellungen in der Praxis zu testen.

4.2.2.2 Webfilter automatisch erstellen

Eine besonders elegante Möglichkeit, solche Webfilter bei aktuellem Bedarf einzurichten, bietet das Dashboard. Stört beim Browsen einer Webseite ein Link oder Objekt, das man in Zukunft am liebsten nicht mehr sehen möchte, so selektiert man das Objekt mit der linken Maustaste und wählt mit der rechten Maustaste im Kontextmenü die Funktion „Kopieren“. Als Beispiel sei wieder ein Foto des Forschungszentrums auf dessen Homepage www.fz-juelich.de ausgewählt:

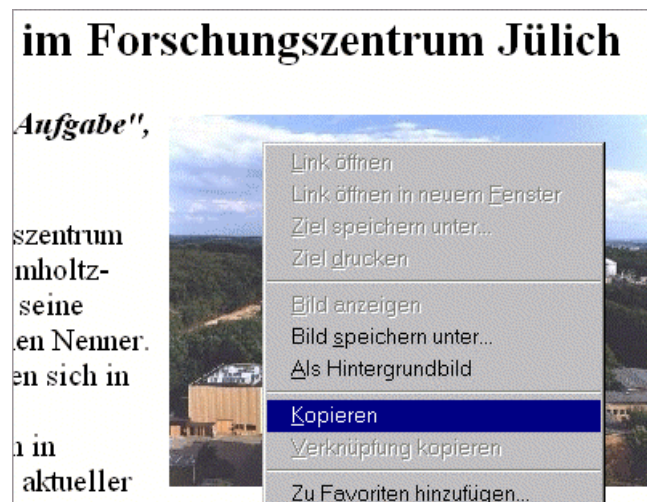



Abbildung 8: Kopieren eines Webobjektes

Anschließend wählt man im Kontextmenü (rechte Maustaste) des Papierkorbsymbols  des Dashboards die Funktion „Paste into Trashcan“ und erhält damit ein weiteres Menü,

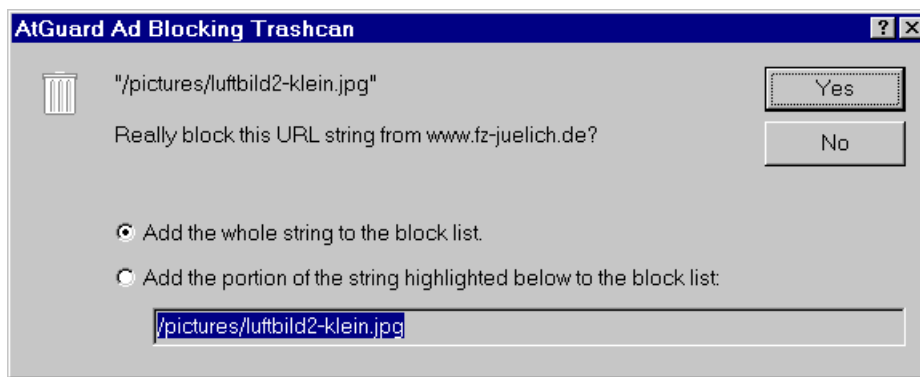


Abbildung 9: Zuordnung zur Filterdomäne

das die Adresse des Webservers und den dort zu sperrenden URL-Teilstring anzeigt. Durch Bestätigen mit „Yes“ wird dann dieser URL-Teilstring entweder spezifisch für diesen Server oder als Default für alle Webdomänen automatisch in die Liste der zu blockierenden Webinhalte eingefügt:



Abbildung 10: Der automatisch erstellte Filtereintrag

Für die Homepage des Forschungszentrums Jülich würde dies bedeuten, daß sie in Zukunft stets ohne dieses spezielle Foto dargestellt würde, während alle anderen Bilder auf allen Webseiten des Forschungszentrums weiter wie üblich dargestellt würden. Im Unterschied zu der in den meisten Browsern verfügbaren Funktion zur einfachen Deaktivierung von Bildinhalten lassen sich mit AtGuard auf diese Weise beliebige HTML-Inhalte Server- und Domänen-spezifisch kontrollieren.

4.2.3 Die Weitergabe lokaler Benutzerinformationen: „Privacy“

Im Untermenü „Privacy“ kann wie bei allen Webfiltern ebenfalls Domänen-bezogen eingestellt werden, welche Daten des lokalen Benutzerprofils der Webbrowser an den Webserver einer Domäne weitergibt. Dies sind einerseits bei früheren Besuchen einer Website lokal gespeicherte „Cookies“, andererseits HTML-Kopfdaten („header fields“), die Informationen über den Browser, das Browsingverhalten des Benutzers oder dessen Email-Adresse an den Server weitergeben. Nach einer Neuinstallation von AtGuard ist der Privacy-Schutz zunächst nicht aktiviert. Dies wird auch im Menü unten durch die Zeile „The Privacy filter is not enabled“ angezeigt. Er kann durch Auswahl des „Cookies“-Kästchens im Dashboard oder wie unten beschrieben im Setup-Menü „Filters“ aktiviert werden.

Cookies sind lokal auf der eigenen Maschine durch den Webserver abgelegte, kleine Dateien ($\leq 4\text{KB}$), die einen Namen, einen URL-Pfad, eventuell ein Gültigkeitsdatum und einige harmlose Textinformationen enthalten. Sie benötigen wenig Platz auf der Festplatte und beinhalten keine Mechanismen zur Ausführung von Programmen oder Makros und sind deshalb für die Sicherheit des Betriebssystems unbedenklich.

Cookies und auch Referer-Felder (Felder 1 und 2), die dem Server die URL derjenigen Seite verraten, von der aus diese Webseite aufgerufen wurde, erlauben jedoch den Webbetreibern das Erstellen von Nutzungsprofilen, die beispielsweise gezielt die Interessen und Vorlieben des Benutzers erfassen und für meist unerwünschte Werbeaktionen durch Email (sog. Spam-

Mail) mißbraucht werden können. Das ist besonders leicht, wenn der Browser die E-Mail-Adresse des Benutzers kennt und diese auf Anfrage an den Server weiterleitet (Feld 4).

Die Preisgabe des eigenen Browsertyps (Feld 3) erlaubt zwar einerseits eine optimale Unterstützung dieses Browsertyps (z.B. durch JavaScript oder ActiveX-Objekte), andererseits gibt er einem möglichen „Hacker“ damit wertvolle Hinweise auf mögliche Angriffspunkte der jeweiligen Browser- und Betriebssystemvariante.

Die vom Hersteller der Software mitgelieferten Voreinstellungen sind als Default für den Besuch fremder, durchschnittlich vertrauenswürdiger Websites sicher geeignet; Cookies und Referer-Informationen werden abgeblockt, und die eigene Mailadresse wird nicht an den Server weitergegeben. Nur der Browsertyp wird mitgeteilt, um diesen optimal bei der korrekten Darstellung der Webinhalte zu unterstützen:

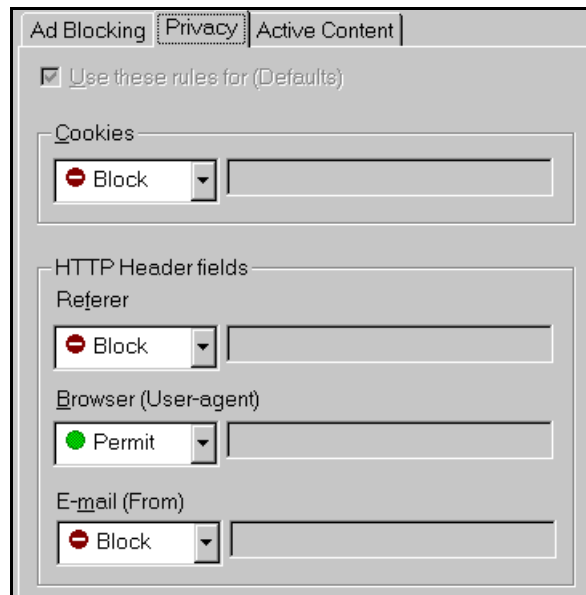


Abbildung 11: Default-Einstellungen für Privacy

Dabei sollte man daran denken, die Einstellungen des „Active Content“ entsprechend zu wählen, da ansonsten der Typ des Browsers einen direkten Hinweis auf Möglichkeiten zum Mißbrauch aktiver Inhalte (Windows Scripting-Technologie, ActiveX , Java) gibt.


Wer sich an einer möglichen Verfolgung seiner Webaktivitäten durch Außenstehende oder an unerwünschter Email an seine Adresse nicht stört, kann ohne Bedenken für die lokale Systemsicherheit alle diese Informationen mit „Permit“ auch freigeben. Dies gilt insbesondere für Webserver im eigenen Intranet. Ersetzen der angeforderten Informationen durch willkürlich definierte Texte mit „Reply“ ist weniger empfehlenswert, da man die Reaktion des Servers auf solche Rückgabewerte nicht kennt und dies unter Umständen zu Kommunikationsproblemen mit dem Server führen kann.

4.2.4 Die lokale Ausführung von Programmen: „Active Content“

Dieses Menü befaßt sich mit Filtereinstellungen, die unmittelbar die Sicherheit des lokalen Systems betreffen: Die Ausführung aktiver Webinhalte, d.h. letztlich die Ausführung fremder Programme auf dem eigenen Rechner, stellt zumindest derzeit noch ein hohes Risiko für die Integrität der Daten und des Betriebssystems dar. Dies trifft – wie leider in der Vergangenheit immer wieder auch bei anderen Betriebssystemen beobachtet – selbst auf Techniken zu, bei denen erhöhte Systemsicherheit ein ursprüngliches Designziel war, die aber auf Grund einer fehlerhaften Implementierung dieses Ziel weit verfehlen (wie beispielsweise die Java-

Sandbox von Windows). Häufig besteht auch ein direkter Widerspruch zwischen der Forderung nach Systemsicherheit und dem Wunsch, Software und Rechner über Netzwerkverbindungen aus der Ferne zu bedienen, ohne dabei auf die lokalen Funktionalitäten des Systems und den gewohnten Komfort zu verzichten.

Das Menü „Active Content“ enthält drei Rubriken für JavaScript, Binärprogramme und animierte Grafiken. Die Grundeinstellungen werden wieder in der Domäne „Defaults“ vorgenommen und enthalten im Zustand der Auslieferung unter „Miscellaneous“ nur ein Filter, das Mehrfachdurchläufe animierter Grafiken wie z.B. der auf vielen Webseiten beliebten „animated GIF’s“ verhindert. Dies schont etwas die Ressourcen des Rechners und die Nerven des Betrachters, wäre aber ansonsten nicht wichtig. Interessant wird dieses Filter allerdings dort, wo von einem X-Terminal oder einem Windows-Terminal aus der Webbrowser auf einem entfernten Server über das Netz benutzt wird. Beispiele dieser Technik sind Wincenter von NCD oder der Windows Terminal Service von NT. In diesem Falle wird jeder einzelne Frame einer animierten Grafik wieder und wieder über das Netz zum Terminal geschickt, was zu einer beträchtlichen, im Grunde unsinnigen Erhöhung der Netzlast führt.

Die Felder 1 und 2 im Untermenü „Script“ betreffen die Ausführung von JavaScript, das Bestandteil fast aller heute angebotenen Webseiten ist. Häufig wird JavaScript zum Erleichtern der Navigation durch farblich hervorgehobene, aktive Schaltknöpfe, durch Aufklappen von Untermenüs oder auch durch Aktivieren zusätzlicher Hilfsfenster benutzt. Wer viel im Web „surft“, kann es sich kaum leisten, die Ausführung von JavaScript ganz zu verhindern, ohne beständig mit Navigationsproblemen oder Fehlermeldungen konfrontiert zu werden. Deshalb ist für solche Anwender zu empfehlen, die Ausführung von JavaScript (Feld 1) zuzulassen. Hingegen kann das Kästchen „Block only popup window script“ (Feld 2) im allgemeinen ohne Probleme deaktiviert werden. Sollte wirklich einmal ein wichtiges Popup-Fenster beispielsweise zur Eingabe eines Paßwortes oder zur Eingabe von Formulardaten benötigt werden, so läßt sich diese Funktion rasch über das Menü „Settings“ reaktivieren, oder man deaktiviert AtGuard momentan durch Anklicken von „Enable AtGuard“ im Symbol  der Taskleiste.

Die Felder 3 und 4 beziehen sich mit „Binary Executables“ auf Programme und ActiveX-Objekte, deren Ausführung vom fremden Webserver angefordert bzw. die auf den PC heruntergeladen und dort lokal ausgeführt werden. Beide Techniken sind derzeit in der Lage, auf Ressourcen des lokalen Betriebssystems wie etwa das Dateisystem zuzugreifen und können daher von Hackern, die selbst einen Webserver betreiben oder einen der etablierten Webserver manipuliert haben, für Angriffe mißbraucht werden. Es ist daher dringen anzuraten, solche aktiven Webinhalte durch Auswahl der Kästchen 3 und 4 zu deaktivieren. Eine sinnvolle Defaulteinstellung für „Active Content“ bei mittleren Sicherheitsanforderungen wäre also wie folgt:

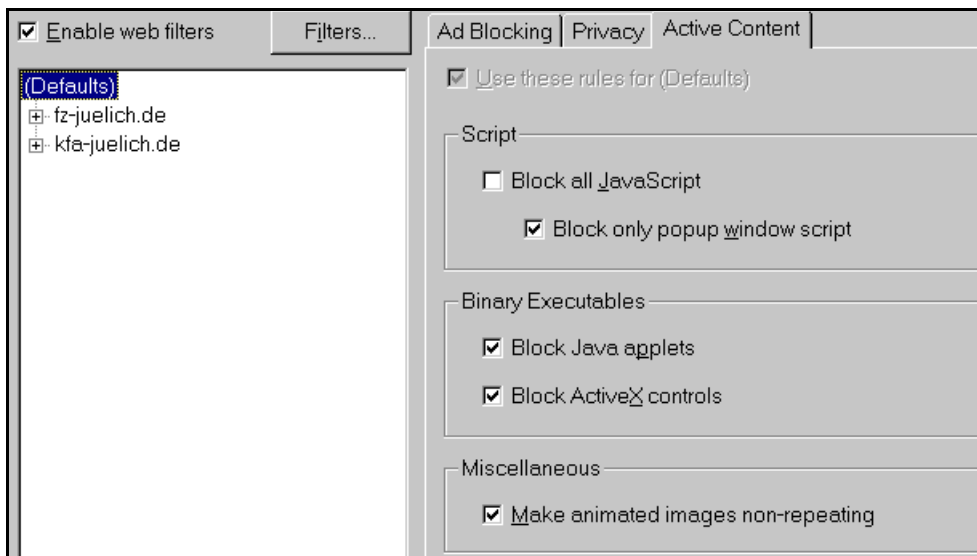


Abbildung 12: Empfohlene Einstellungen für „Active Content“

Auch hier gilt wieder, daß man bei vertrauenswürdigen Servern kurzzeitig den Filter deaktivieren, oder besser bei häufigerem Besuch eines solchen Servers diesen explizit in die Domänenliste eintragen und mit „Use these rules for (Defaults)“ gesondert konfigurieren kann. Man sollte sich dabei allerdings bewußt sein, daß durch eine eher schwierige und daher seltene Manipulation von Nameservern im Internet auch die Identität eines Webserver vorgetäuscht werden kann („Masquerading“), solange dieser keine gesicherte, authentifizierte Verbindungstechnik benutzt. Allerdings ist die Gefahr einer solchen Manipulation so gering einzuschätzen, daß der Wert einer domänenspezifischen Filterkonfiguration hierdurch nicht geschmälert wird.

4.2.5 Globale Webfilter-Optionen: „Filters...“

Neben dem Kästchen zur Aktivierung oder Deaktivierung aller Webfilter im Menü „Web“ findet sich der Knopf „Filters...“, über dessen Untermenü weitere, globale Webfiltereinstellungen vorgenommen werden können:

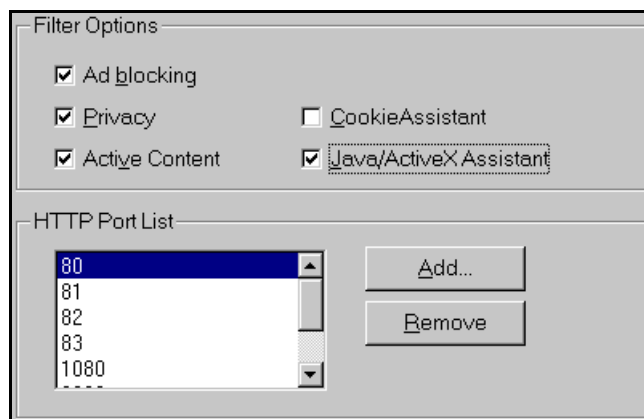


Abbildung 13: Globale Webfilter-Optionen

4.2.5.1 Die HTTP Port-Liste

Um Webfilter überhaupt sinnvoll und ohne großen Zeitverlust durch eine Analyse aller Dateninhalte anwenden zu können, muß das Programm wissen, über welche IP-Portnummern („Dienste“) der Browser sich an einen Webserver wendet. Standard ist der Port 80, es werden aber häufig für Server, deren Inhalte nicht öffentlich z.B. durch Suchmaschinen bekannt ge-

macht werden sollen, beliebige andere Portnummern wie etwa die recht beliebten Portnummern 8080 oder 8001 benutzt. Solche zusätzlichen Portnummern für eigene, nicht den Standard 80 benutzenden Webserver können im Untermenü „HTTP Port List“ mit „Add“ der Liste der HTTP-Ports hinzugefügt oder mit „Remove“ wieder aus dieser Liste entfernt werden.

4.2.5.2 Filter-Optionen und -Assistenten

Das Untermenü „Filter Options“ erlaubt, die oben dokumentierten Filter für „Ad Blocking“, für „Privacy“ und für „Active Content“ global, d.h. ohne Berücksichtigung der individuellen Domänenkonfiguration, ein- oder auszuschalten. Die erstgenannten beiden Filter können auch bequemer im Dashboard mit „Ads“ bzw. „Cookies“ an- und abgeschaltet werden. Es versteht sich von selbst, daß diese Filter im Normalfall alle eingeschaltet bleiben müssen, will man nicht auf Webfilter generell verzichten. Von der Logik der Bedienung wären diese Auswahlkästchen wohl besser auf den Untermenüs für die Default-Einstellungen der Webfilter untergebracht.

Eine besondere Eigenschaft des AtGuard sind seine Assistenten. Das sind Popup-Menüs, die es erlauben, beim Zugriff auf neue Domänen oder Webserver für Inhalte, für die noch keine Filterkonfiguration definiert wurde, diese schnell und interaktiv zu erstellen. Sind beispielsweise die Filter für aktive Inhalte und das Kästchen „Java/ActiveX Assistant“ aktiviert (es müßte entsprechend der tatsächlichen Funktion präziser „Scripting/Java/ActiveX“ heißen), so erscheint beim Zugriff auf die Seite des Microsoft-Servers „www.microsoft.com“ ein Popup-Menü, das die Verwendung von JavaScript auf der Microsoftseite anzeigt und dazu auffordert, entweder für die ganze Domäne „microsoft.com“ oder nur für diesen bestimmten Server „www.microsoft.com“ die Ausführung von JavaScript zu blockieren oder zuzulassen:

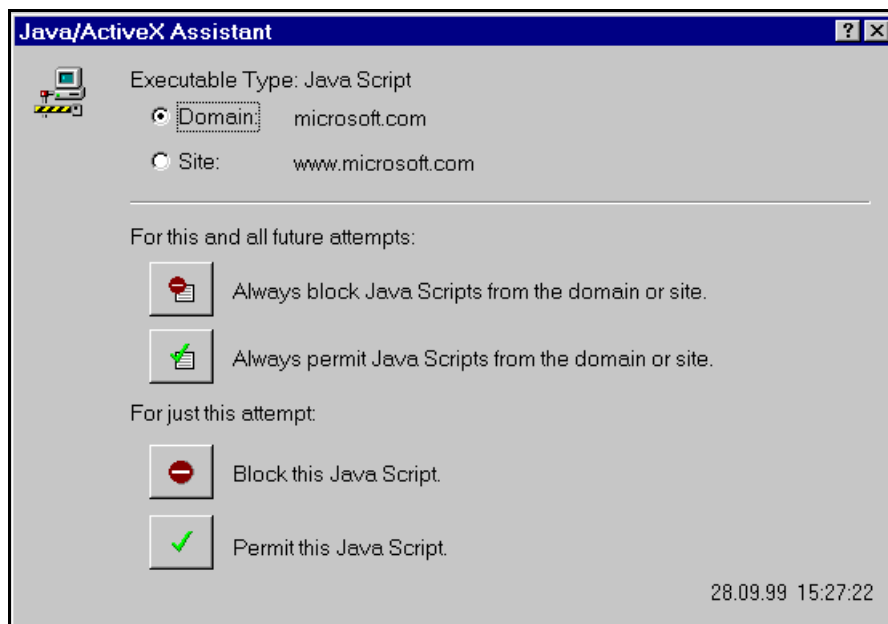


Abbildung 14: Der Assistent für Java/ActiveX

Diese Entscheidung kann im Untermenü „For just this attempt“ einmalig für genau diesen Seitenzugriff oder unter „For this and all future attempts“ auch für alle zukünftigen Zugriffe auf diese Domäne oder diesen Server gefällt werden. Im letztgenannten Fall wird dann automatisch ein entsprechender Eintrag in der Domänenliste der Webfilter für „Active Content“ eingerichtet.

Einen ähnlichen Assistenten bietet AtGuard mit dem „CookieAssistant“ auch für die Einträge in der Rubrik „Privacy“. Die Benutzung dieser Assistenten ist vor allem dann angebracht,

wenn man immer wieder auf eine begrenzte Zahl wohlbekannter Server zugreift. Für diese richtet man dann mit Hilfe der Assistenten oder durch manuelle Eingabe die gewünschte Filterkonfiguration ein und benutzt die Assistenten nur für den seltenen Fall eines Zugriffs auf einen fremden Server. Wer z.B. bei der Suche nach bestimmten Informationen häufig auf rasch wechselnde Server im Internet zugreifen muß, ist mit einer festen Default-Konfiguration und mit abgeschalteten Assistenten besser beraten. Eine weitere, manchmal recht informative Anwendung der Assistenten ist, sie temporär als Testwerkzeug für die Art der von einem unbekanntem Server übertragenen Webinhalte zu benutzen.

4.3 Der Firewall und die Regelerstellung

4.3.1 Die Funktionsweise des Firewalls

Der sicher interessanteste Aspekt von AtGuard ist die Funktion als Firewall, dessen Konfiguration sich im Menü „Settings“, Untermenü „Firewall“ erschließt. Zunächst kann hier mit der Auswahl „Enable Firewall“ die Gesamtfunktion von AtGuard als Firewall aktiviert oder deaktiviert werden“. Hat man einmal Probleme mit der Kommunikation und möchte sicherstellen, daß nicht irgendeine Fehlkonfiguration des Firewalls Ursache dieser Schwierigkeiten ist, so läßt sich der Firewall mit dem entsprechenden Auswahlkästchen im Dashboard schnell temporär außer Funktion setzen. Die Konfiguration und die Funktion der Webfilter wird hierdurch nicht beeinflußt!

Mit dem Auswahlkästchen „Enable RuleAssistant (interactive learning mode)“ wird ähnlich wie bei den oben beschriebenen Webfiltern ein Assistent aktiviert, der sich allerdings funktionell von diesen unterscheidet und im Verbund mit einem sorgfältig ausgewählten Regelsatz ein wirklich nützliches Werkzeug zur Überwachung und Kontrolle der eigenen Kommunikation und insbesondere der von außen an den PC herangetragenen Kommunikationsversuche darstellt.

Jeder IP-Kommunikation liegt der gleiche „IP-Socket“-Mechanismus zu Grunde: Ein IP-Paket wird von einem „Client“ mit Angabe seiner IP-Quelladresse und einer Portnummer (Client Port) an einen „Server“ gesandt, auf dem ein bestimmtes Programm („Dienst“ unter Windows NT, „daemon“ unter Unix) mit der IP-Adresse des Servers und einer durch die Art des zu erbringenden Dienstes festgelegten Portnummer (Service Port) lauscht. Quell- und Zieladressen, die beteiligten Portnummern und die auf dem Serverport aktive Applikation (beispielsweise ein Webserver) sind die charakterisierenden Eigenschaften einer IP-Verbindung. Das Internet Control Message Protocol ICMP ist integrierter Bestandteil des IP-Protokollstacks und kennt nur einfache Steuerbefehle wie z.B. „Echo Request“ und „Echo Reply“ (Ping).

Das Prinzip des Firewalls besteht darin, für jedes IP-Paket und seit der Version 3.2 von AtGuard auch für ICMP-Protokollpakete deren Eigenschaften zu analysieren und mit einer Liste vordefinierter Regeln zu vergleichen:

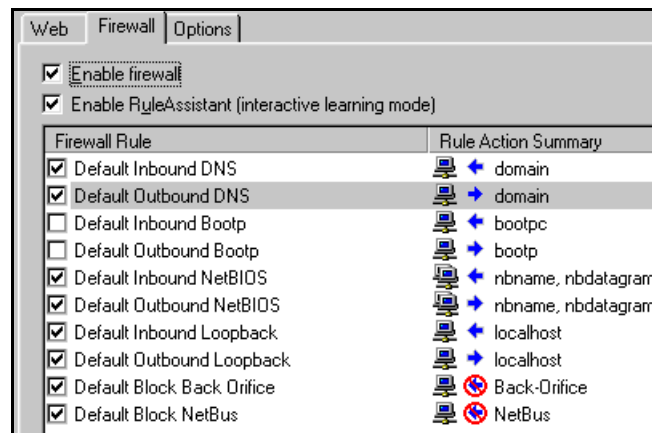


Abbildung 15: Die Default-Konfiguration des Firewalls

Trifft eine der Regeln in allen Eigenschaften zu, so wird die durch die Regel definierte Aktion ausgelöst. Wird keine gültige Regel gefunden, so wird entweder der Regelassistent des interaktiven Lernmodus gestartet oder, falls dieser deaktiviert ist, die Verbindung per Default abgelehnt.

Im Regelfenster wird jede Filterregel in einer Zeile mit einem Schaltkästchen zu ihrer Aktivierung bzw. Deaktivierung, einer möglichst sprechenden Bezeichnung für die Regel, einem Symbol mit Anzeige der Kommunikationsrichtung („Inbound“ oder „Outbound“) und einer Aufzählung der betroffenen Dienste angezeigt. Bei eingeschaltetem Firewall werden diese Regeln **sequentiell von oben nach unten durchlaufen** und abgeprüft. Sobald eine "passende" Regel gefunden wird, wird diese angewandt und alle folgenden Regeln der Liste werden ignoriert.

Wie bereits erwähnt, werden alle nicht explizit durch eine Regel erfaßten Verbindungen kommentarlos blockiert, falls der Regelassistent nicht aktiviert ist. Dies kann zu schwer erkennbaren Fehlern in der Kommunikation führen, wenn der Regelsatz nicht genau den tatsächlichen Anforderungen entspricht. Eine solche Konfiguration ist deshalb **nicht** zu empfehlen. Sie würde darüber hinaus auch das Erkennen unerwarteter oder unbeabsichtigter Kommunikationsversuche mit dem eigenen PC verhindern.

Die in Bild 15 gezeigten Regeldefinitionen werden bei Installation der Software automatisch eingerichtet. Sie stellen einen Minimalansatz an Regeln dar, wie er im allgemeinen – mit Ausnahme des BOOTP-Protokolls – in einem typischen IP-Netz benötigt wird. Diese Regeln werden jedoch in einem komplexeren Netzwerk wie JuNet für eine individuelle Konfiguration einerseits nicht ausreichen, andererseits jedoch stellen sie durch die freizügige Öffnung der NETBIOS-Dienste bereits ein gewisses Risiko dar. Auf diese Thematik wird weiter unten noch genauer eingegangen.

4.3.2 Die manuelle Erstellung von Regeln

Neue Regeln können mit „Add“ der Liste hinzugefügt, mit „Modify“ verändert und mit „Remove“ auch wieder gelöscht werden. Das Löschen entfernt die Regeldefinition unwiederbringlich aus der Liste, während das Deaktivieren einer Regel mit dem Auswahlkästchen die Definitionen beibehält, die Regel selbst aber unwirksam macht.

Die Eigenschaften einer IP-Verbindung, die AtGuard überprüft und die deshalb für die Erstellung einer neuen Regel spezifiziert werden müssen, seien am Beispiel einer Regel für den Zugriff aus JuNet auf einen lokal auf dem PC laufenden Microsoft Peer Webserver erläutert (das Beispiel ist auch deshalb von praktischen Interesse, weil dieser Webserver als Bestandteil

von Windows 98 oder Windows-NT-Workstation im Gegensatz zum Internet Information Server ISS selbst keine Einstellungen der Zugriffssicherheit erlaubt):

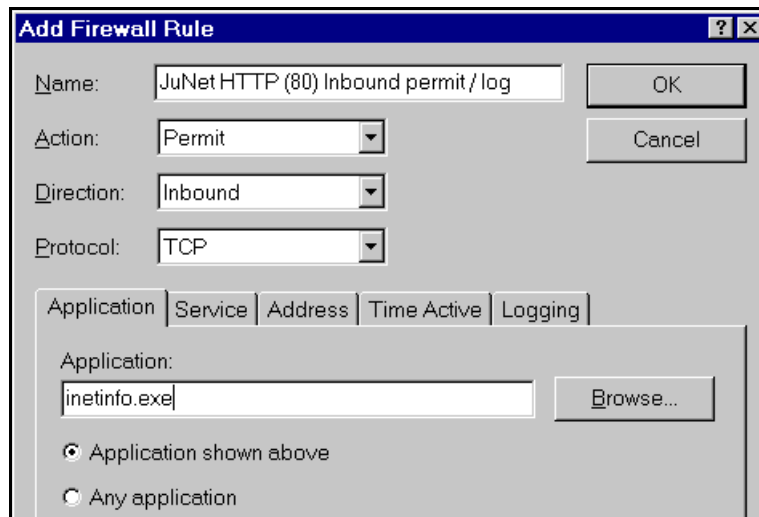


Abbildung 16: Erstellen einer neuen Regel von Hand

1. Name: Das erste Feld enthält einen Namen für die neue Regel. Dieser kann zwar willkürlich gewählt werden, man erkennt jedoch im Laufe der Zeit sehr schnell, daß die Einhaltung einer selbstgewählten Konvention sehr dazu beiträgt, im wachsenden Regelwerk die Übersicht zu behalten. Der Name sollte zweckmäßigerweise folgende Parameter enthalten:

- Name des Rechners oder des Netzes, auf das sich die Regel bezieht (JuNet)
- Art des Dienstes oder Sammelbegriff der Dienste (HTTP).
- Kommunikationsrichtung (Inbound). Wird der Einfachheit halber die Kommunikation nach außen (Outbound) immer erlaubt, so kann dieser Hinweis entfallen.
- Aktion (Block, Permit oder Ignore)
- Zusätzliche Kennungen wie. z.B. „/log“, für Logging oder „/timed“ für zeitliche Einschränkungen der Gültigkeit.

In unserem Beispiel „JuNet HTTP (80) Inbound permit / log“ heißt das, daß alle Rechner aus dem gesamten JuNet auf den Standardport 80 des Microsoft Peer Webservers dieses PCs zugreifen können, und daß diese Zugriffe (zusätzlich zum hoffentlich eingeschalteten Log des Webservers selbst) im Event-Log des Firewalls vermerkt werden.

2. Action: Die IP-Verbindung wird entweder abgeblockt („Block“) oder zugelassen („Permit“). Es gibt eine dritte Einstellung „Ignore“, bei der das Datenpaket ignoriert, aber dennoch im Firewall-Log gezählt wird. In diesem Falle wird auch die Regelliste nach weiteren gültigen Regeln für diesen Verbindungstyp durchsucht.

3. Direction: Hier wird angegeben, ob das Filter für einlaufende („Inbound“), auslaufende („Outbound“) IP-Pakete oder für Pakete in beiden Richtungen („Either“) gelten soll.

4. Protocol: Der Typ des verwendeten IP-Protokolls (das verbindungslose „UDP“, das verbindungsorientierte „TCP“ oder beides, oder das Internet Control Message Protocol ICMP, das zum Beispiel für das „Ping“-Kommando benutzt wird). Es ist wichtig darauf zu achten, daß manchmal identische IP-Ports für unterschiedliche Applikationen benutzt werden, die sich nur in dem Typ des verwendeten Protokolls unterscheiden. Port 513 ist hierfür ein Beispiel: Port 513/UDP ist der „rwho“-Dienst, der Auskunft über im Netz aktive Benutzer gibt,

während 513/TCP für den interaktiven Zugang mittels des „remote login“-Protokolls benutzt wird.

5. Application: Das Programm auf dem lokalen PC, an das sich die Verbindungsaufforderung oder das IP-Paket richtet. Mit SYSTEM werden Applikationen gekennzeichnet, die integrierter Bestandteil des Betriebssystems selbst sind wie beispielsweise der Internet-Nameservice (DNS). In unserem Beispiel richtet sich der HTTP-Request an den Peer Webserver

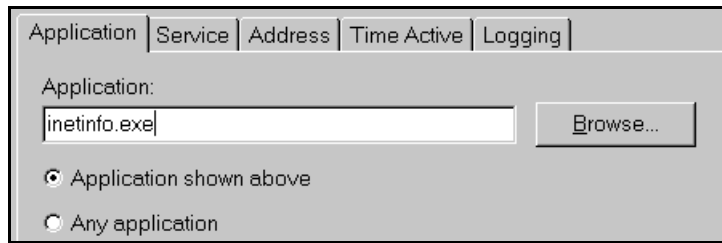


Abbildung 17: Festlegen einer bestimmten Applikation

inetinfo.exe, der folglich als Applikation eingetragen werden kann. Im allgemeinen ist jedoch die Applikation, die einen bestimmten Port wie etwa den Port 80 eines Standard-Webserver bedient, eindeutig und nur einmal aktiv, so daß sich die Angabe der Applikation meist erübrigt und genau so gut „Any application“ gewählt werden kann.

6. Service: Der Name eines IP-Dienstes oder eine IP-Portnummer, die die Art des Dienstes kennzeichnet. Jedes Betriebssystem, das die IP-Protokolle verwendet, besitzt zumindest auszugswise eine Liste der in RFC1700 („Assigned Numbers“) festgelegten Dienste und ihrer zugehörigen Portnummern. Unter Windows NT liegt diese Liste beispielsweise unter C:\%SystemRoot%\system32\drivers\etc\Services. Zusätzlich zu dieser systemeigenen Tabelle standardisierter Ports führt AtGuard noch eine eigene interne Liste, die im Anhang dokumentiert ist. Alle diese Namen können auch bei der Regelerstellung an Stelle der wenig sprechenden Portnummern benutzt werden.

Auch hier muß man die Portnummer eines Dienstes auf dem entfernten Rechner („Outbound“) oder die eines Dienstes auf dem eigenen PC („Inbound“) unterscheiden. Im Falle unseres Beispiels richtet sich die Dienstanfrage an den Webserver auf Port 80 des lokalen PCs, der als „Single service“ mit dem Dienstenamen „http“ eingetragen wird:

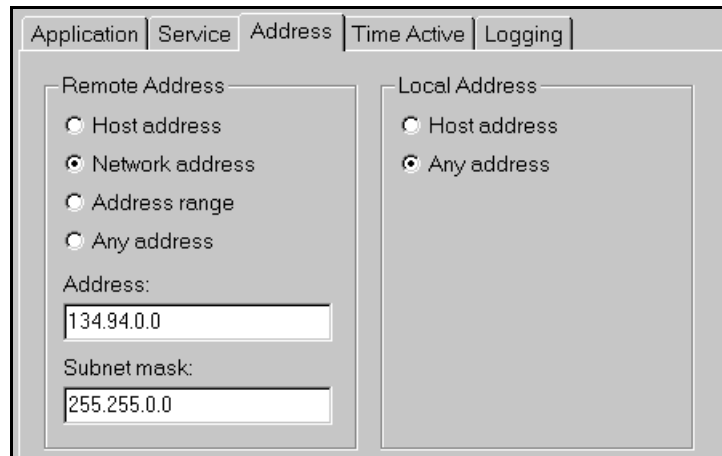


Abbildung 18: Die Definition der Serviceports

Statt eines einzelnen Dienstes können hier auch mehrere Dienste mit Portnummern oder Namen eingetragen werden. Beispiele sind etwa NETBIOS, das die Dienste „nname, nbdagram und nbssession“ benutzt oder Systeme mit zusätzlichen Serverports zur Steuerung oder zur dynamischen HTML-Erzeugung wie zum Beispiel das Managementwerkzeug WhatsUpGold oder das beliebte WebCam32.

7. Address: Dies sind die Internet-Adressen der beteiligten Systeme, entweder in der üblichen „dotted decimal notation“ (134.94.100.71), oder als Internet-Domainname (www.fz-juelich.de). Die „Remote Address“ ist die IP-Adresse des Kommunikationspartners oder ein ganzer Bereich von Adressen, auf den eine Regel sich bezieht. Die „Local Address“ ist die IP-Adresse des eigenen PCs. Besitzt der PC mehrere Netzadapter oder mehrere virtuelle IP-Adressen auf einem Adapter, so kann dies mit dem Eintrag „Any address“ berücksichtigt werden.

Im vorliegenden Beispiel sollen nur Rechner aus dem Adreßbereich von JuNet (wozu auch die externen Netzzugänge über die Modemserver des Forschungszentrums zählen) auf den Webserver zugreifen können, so daß hier



The image shows a dialog box with five tabs: Application, Service, Address, Time Active, and Logging. The 'Address' tab is selected. It is divided into two sections: 'Remote Address' and 'Local Address'. Under 'Remote Address', there are four radio buttons: 'Host address', 'Network address' (which is selected), 'Address range', and 'Any address'. Below these are two text input fields: 'Address:' containing '134.94.0.0' and 'Subnet mask:' containing '255.255.0.0'. Under 'Local Address', there are two radio buttons: 'Host address' and 'Any address' (which is selected).

Abbildung 19: Spezifikation einer Netzwerkadresse

als „Remote Address“ die Netzwerkadresse **134.94.0.0** von JuNet mit der Netzmaske **255.255.0.0** eingetragen werden muß. Für den lokalen PC mit nur einem Netzwerkinterface kann dessen IP-Adresse oder ebenso gut „Any address“ angegeben werden.

8. Time Active: Hier kann für jede Regel separat eingetragen werden, für welchen Wochentag und Zeitraum die Regel aktiv sein soll. Es läßt sich pro Wochentag und Regel jeweils ein festes Zeitintervall definieren. Damit lassen sich bestimmte Dienste zeitgesteuert anbieten, oder es läßt sich außerhalb der regulären Arbeitszeit die Sicherheit des Systems vor den häufig „nachtaktiven“ Hackern deutlich erhöhen. Als Beispiel sei ein Gültigkeitszeitraum von 8 bis 17 Uhr täglich angenommen. Außerhalb dieser Zeit würde die Regel nicht gelten, und die Verbindung würde deshalb per Default abgelehnt (vorausgesetzt, sie wurde nicht versehentlich durch eine in der Liste voranstehende Regel bereits erlaubt!). Die Auswahl der Zeit erfolgt durch Anklicken der Uhrensymbole rechts neben der Zeitanzeige und kann für jeden Tag einzeln oder für die ganze Woche übernommen werden:

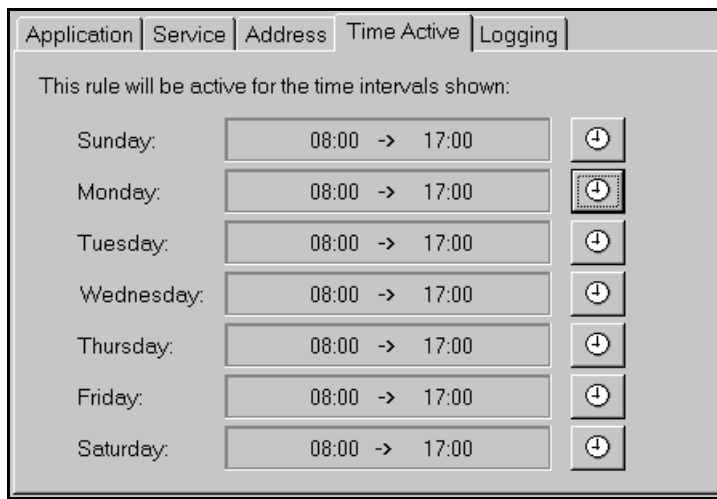


Abbildung 20: Einstellen der Gültigkeitszeiten einer Regel

9. Logging: Jedes Ansprechen einer Firewallregel kann mit den Details der IP-Verbindungsanforderung im Eventlog aufgezeichnet werden. Wahlweise kann der Logeintrag aber auch erst erfolgen, wenn eine bestimmte Anzahl an IP-Paketen beobachtet wurde, auf die diese Regel zutrifft.

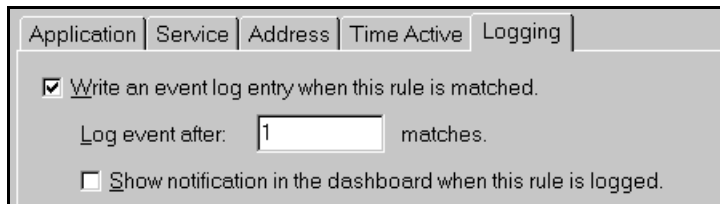



Abbildung 21: Loggen einer Regel

Das untere Auswahlkästchen aktiviert eine Alarmanzeige in Form eines roten Symbols, das beim Ansprechen dieser Regel links neben dem kleinen Mülleimer  im Dashboard erscheint. Dies wird allerdings leicht übersehen, da kein zusätzliches akustisches Signal auf den Regelalarm hinweist.

Hat man die Vermutung, daß bestimmte Zugriffe auf den eigenen PC versucht werden, die man vielleicht nicht einmal verhindern, die man aber sehr wohl registrieren möchte, so empfiehlt sich hierfür die Erstellung einer eigenen Regel mit Logging. Das ist weniger lästig als das wiederholte Bedienen des Regelassistenten, der bei jedem Verbindungsversuch als Pop-up-Fenster den Gang der Arbeit stört. Die Regel selbst kann einmalig mit Hilfe des Regelassistenten erstellt und anschließend manuell das Logging aktiviert werden.

4.3.3 Die halbautomatische Regelerstellung mit dem Regelassistenten

Eine Besonderheit von AtGuard ist der schon mehrfach erwähnte interaktive Regelassistent, der im Setup durch "Enable Rule Assistant (interactive learning mode)" aktiviert wird. Bei jedem neuen IP-Verbindungstyp, der nicht von einer bereits vorhandenen Regel abgedeckt wird, wird dieser Assistent automatisch aufgerufen und erscheint unübersehbar als Pop-up-Fenster auf dem Bildschirm des PC. Er erlaubt menügesteuert die Definition einer neuen Regel, wobei die wichtigsten Parameter der verursachenden Verbindungsanfrage bereits eingetragen sind und durch Bestätigen übernommen oder direkt modifiziert werden können. Das folgende Beispiel zeigt einen Verbindungsversuch der Maschine „zam329“ zu einem auf dem PC laufenden FTP-Server, dem bekannten WAR-FTP-Server „war-ftp.exe“:

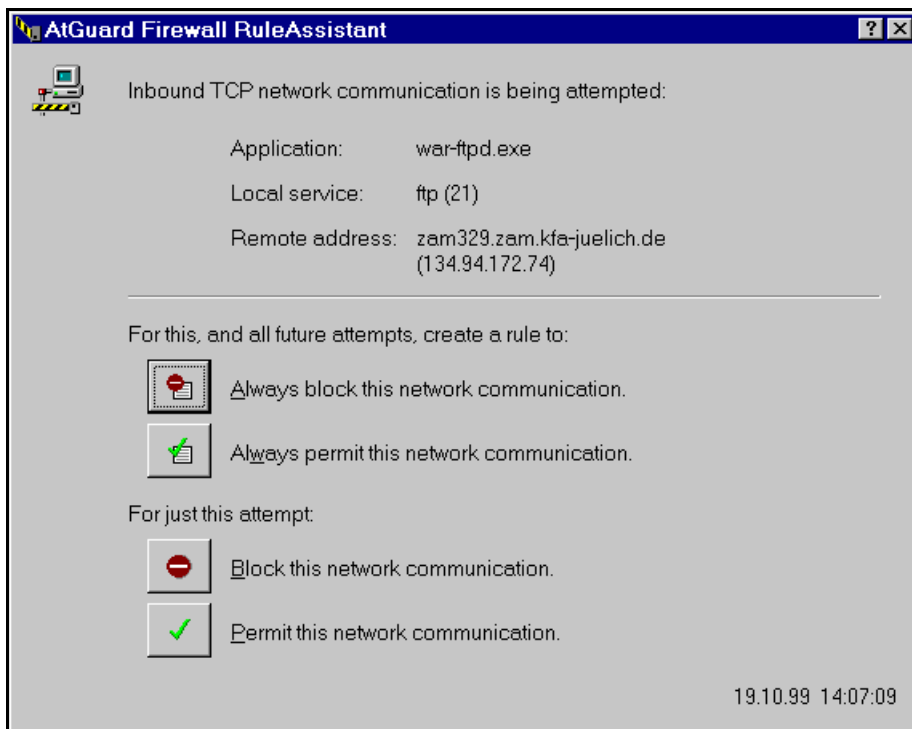


Abbildung 22: Ein FTP-Verbindungsversuch im Fenster des Regelassistenten

Wie bei den oben beschriebenen „Wizards“ für Webfilter kann diese Verbindungsanforderung momentan „for just this attempt“ abgelehnt oder akzeptiert werden und wird mit einem entsprechenden Eintrag im Eventlog registriert:

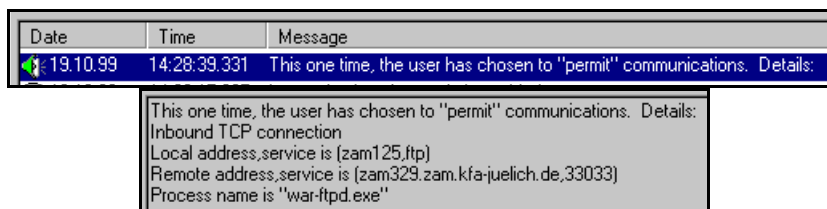


Abbildung 23: Der Eintrag im Eventlog durch den Regelassistenten

Interessanter ist die Möglichkeit, mit den oberen beiden Knöpfen „for this and all future attempts“ eine neue, permanente Regel für diesen Verbindungstyp zu definieren. Mit „always permit this network communication“ führt der Assistent zum nächsten Menüpunkt „Create Permit Rule“, in dem zunächst nochmals eine Zusammenfassung der Verbindungsdaten angezeigt wird. Bestätigen mit „Weiter“^{*)} führt zum nächsten Definitionsschritt, in dem die erkannte Zielapplikation „war-ftp.exe“ oder allgemein „Any application“ zur Auswahl angeboten werden:

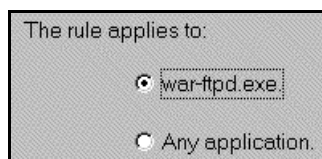


Abbildung 24: Bestätigung der Applikation

^{*)} die Beschriftungen der Knöpfe entstammen den deutschsprachigen Windowsklassen des lokalen PCs, während die Meldungen von AtGuard selbst Bestandteil des englischsprachigen Programms sind.

Im vorliegenden Fall soll die Kommunikation zu Port 21, der Kontrollverbindung des FTP-Servers, auf genau diese Applikation beschränkt bleiben, da dieser Server im Gegensatz zu anderen wie beispielsweise dem FTP-Server der „Peer Web Services“ von Microsoft sehr viel bessere Sicherheits- und Kontrollmechanismen bietet.

Im folgenden Fenster wird mit

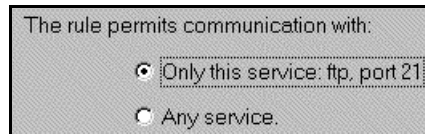


Abbildung 25: Bestätigung des Service-Ports (FTP-Kontrollverbindung)

der Zielport der FTP-Kontrollverbindung, Port 21 mit „Weiter“ bestätigt. Der Assistent bietet hier nur die Auswahl des tatsächlich durch diese Verbindungsanforderung gewünschten Zielports oder aber „Any service“. Eine detailliertere Liste möglicher Dienste kann nur wie oben beschrieben durch nachträgliche Modifikation der mit Hilfe des Assistenten erstellten Regel von Hand eingegeben werden.

Folgerichtig wird als nächstes die IP-Adresse der Maschine angeboten, von der die Verbindungsanforderung ausging:





Abbildung 26: Quelladresse der Verbindungsanforderung

Auch hier kann wieder nur genau diese Adresse oder „Any address“ angegeben werden; Modifikationen wie zum Beispiel die Angabe einer Netzwerk- statt einer einzelnen Maschinenadresse sind nur nachträglich von Hand möglich.

Zuletzt wird nochmals eine Zusammenfassung der zu erstellenden Regel angezeigt, die im ersten Feld mit einem sprechenden Namen (siehe Absatz 4.3.2) versehen und mit „Fertigstellen“ unten an die Liste der vorhandenen Regeln angehängt werden kann:



Abbildung 27: Die mit dem Reglassistenten erstellte neue Regel

Wegen der sequentiellen Abarbeitung der Regeln ist darauf zu achten, daß eine solche Regel „unten in der Liste“ nicht später versehentlich durch eine umfassendere Regel weiter oben in der Liste unwirksam gemacht wird. Beispiel wäre eine Regel, die generellen Zugang für die Maschine zam329 erlaubt, womit ebenfalls ein FTP-Zugang über einen anderen als den Port 21 oder zu einem anderen Server als dem WAR-FTP auf Port 21 erlaubt wären. Aus diesem Grunde lassen sich die Regeln in der Liste mit Hilfe der Knöpfe  oder  im Menü „Settings“ geeignet sortieren, beispielsweise in der Reihenfolge von spezifischeren zu allgemeiner gefaßten oder von häufig benutzten zu selten aktivierten Regeln. Beim Sortieren einer wachsenden Anzahl an Regeln ist die Einhaltung der obenerwähnten oder ähnlicher Namenskonventionen dringend anzuraten. Die Praxis zeigt, daß die Regelliste je nach Kommunikationsumfeld und eigenem Kommunikationsverhalten schnell auf zehn, zwanzig oder mehr Regeln anwächst, deren logische Konsistenz von Zeit zu Zeit überprüft und sichergestellt werden muß.

4.3.4 Testen einer Regel

Das Menü für die Definition der Firewall-Regeln bietet mit dem Knopf „Test...“ eine Möglichkeit, die Wirksamkeit einer explizit erstellten oder der als „implizit“ gekennzeichneten Default-Regel zu testen. Hierzu wird die zu testende Verbindungsanforderung an den At-Guard-Treiber simuliert, ohne daß hierzu der Firewall aktiviert sein muß. Wird eine „passende“ Regel gefunden, so wird diese im Testfenster angezeigt und automatisch in der Regelliste selektiert. Ein Beispiel eines solchen Tests zeigt die folgende Abbildung,

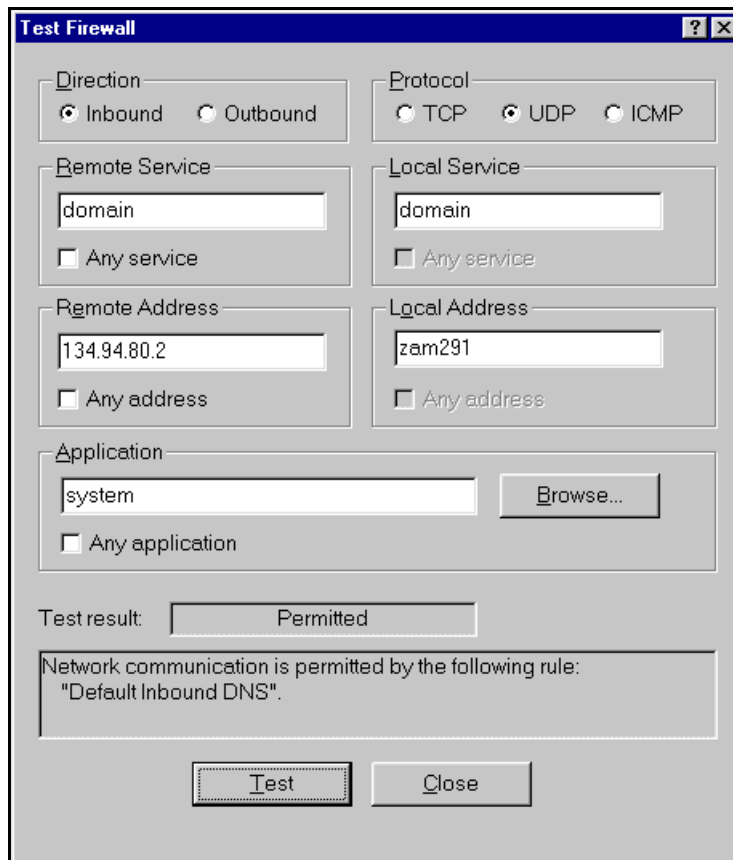


Abbildung 28: Test einer Firewall-Regel

bei der untersucht wurde, ob der Nameserver im JuNet (Adresse 134.94.80.2) ungehindert mit den Systemdiensten für die IP-Namensauflösung des lokalen PCs zusammenarbeiten kann. Der Test ergibt erwartungsgemäß, daß dies durch die Regel „Default Inbound DNS“ gewährleistet wird.

5 Event-Log und Statistik

5.1 Das Event-Log

Alle Ereignisse wie Verbindungsaufbau, gefilterte Webinhalte oder angesprochene Firewall-Regeln werden (falls bei der Regelerstellung entsprechend konfiguriert) im Event-Log mit einem Zeitstempel versehen abgespeichert:

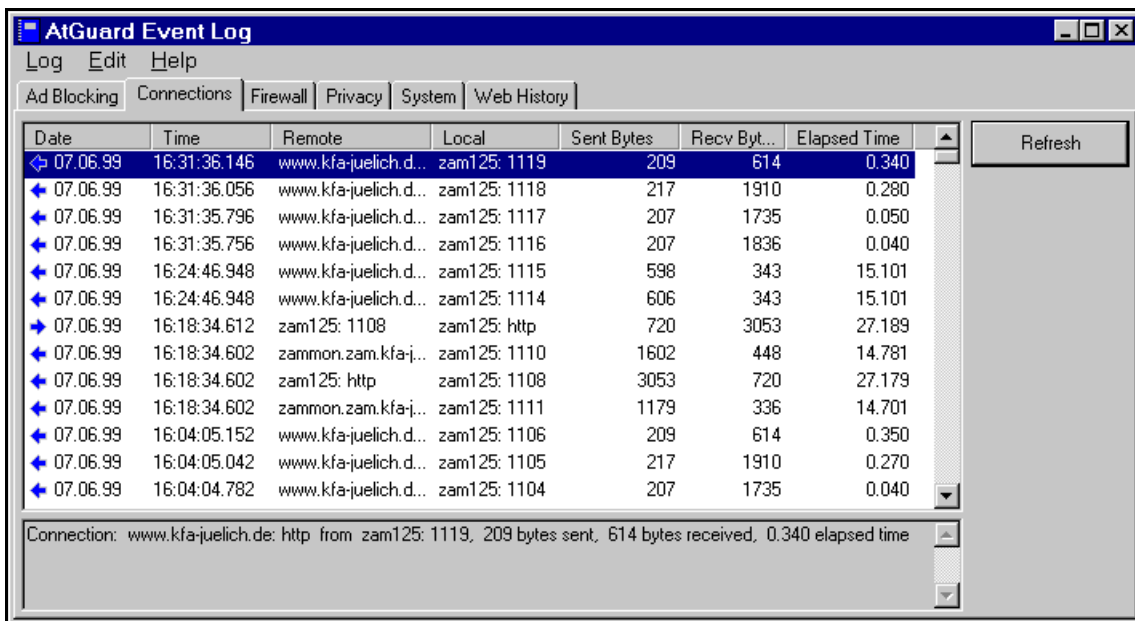


Abbildung 29: Das Event-Log mit der Anzeige der IP-Verbindungen

Im Ordner „Ad Blocking“ können die gesperrten Werbeinhalte eingesehen werden,

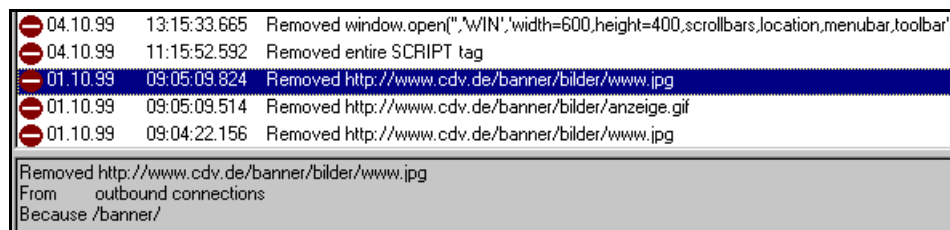


Abbildung 30: Anzeige der gesperrten Webinhalte

wie etwa im Beispiel der Abb.29, als am 4.10. nacheinander ein Popup-Fenster und ein JavaScript-Tag und am 1.10.einige Reklamebilder unterbunden wurden. In der Detailbeschreibung im unteren Teil des Logfensters wird zur Kontrolle noch das Textmuster „/banner/“ angezeigt, auf Grund dessen ein selektiertes HTML-Objekt aus der Seite entfernt wurde.

Der Ordner „Connections“ zeigt die IP-Verbindungen mit Richtung, Datenraten und Zeitdauer wie in Abb. 29 dargestellt. Die aktuell aktiven Verbindungen werden wie oben beschrieben im Dashboard angezeigt und mit etwas zeitlicher Verzögerung in das Event-Log eingetragen.

Im Ordner „Firewall“ werden Start und Stopp der Firewallfunktion sowie die Verbindungsdetails solcher Anforderungen angezeigt, für die eine Firewallregel mit der Option „Logging“ angesprochen hatte. Außer diesen permanenten Regeln werden auch die einmaligen Aktionen des Regelassistenten „for just this attempt“ hier eingetragen und mit einem besonderen Symbol (grüner Lautsprecher) gekennzeichnet:

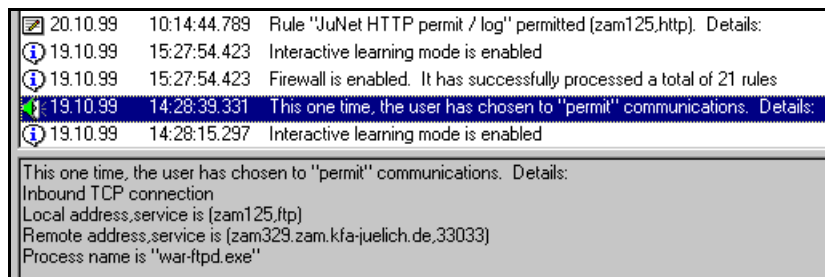


Abbildung 31: Die Anzeige aktivierter Regeln des Firewalls

Der Ordner „Privacy“ zeigt die Auswirkung der Webfilter, also beispielsweise

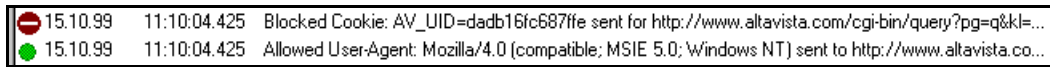


Abbildung 32: Loggen von Privacy-Ereignissen


das Sperren eines Cookies vom und die Weitergabe des Browsertyps an den Webserver.

Die beiden letzten Ordner „System“ und „Web history“ enthalten weniger sicherheitsrelevante Informationen, die Web-Historie als Liste der besuchten URL's steht – soweit diese nicht durch ein Filter unterbunden wurden – ebenfalls in jedem Browser z.B. als „Verlauf“ zur Verfügung.

Das Pulldown-Menü "Log" bietet einige nützliche Zusatzfunktionen, um Ereignis-Einträge der einzelnen Ordner als Textdateien abzuspeichern, auszudrucken, oder sie beispielsweise nach jeder Abmeldung vom System automatisch zu löschen. Letzteres empfiehlt sich kaum, da man doch in regelmäßigen Abständen vor allem die Einträge in den Rubriken „Connections“ und „Firewall“ kontrollieren und auf Hinweise für unerwartete Ereignisse oder fehlerhafte Konfiguration des Firewalls überprüfen sollte.

Mit „Change Tab File Size“ im Pulldown-Menü „Log“ läßt sich die maximale Dateigröße der Ereignislogs in jeder Rubrik getrennt einstellen (Default ist 128k). Nach Erreichen dieser Maximalgröße werden ältere Ereignisse aus dem Log gelöscht (FIFO-Prinzip).

5.2 Die Verbindungsstatistik

Mit dem Menüpunkt „Statistics“ im Symbol  der Taskleiste oder im Pulldown-Menü des Dashboards wird eine grafische Darstellung der Summen- und Verkehrsstatistiken aktiviert. Die Daten werden in verschiedene Gruppen unterteilt dargestellt:

- Netzwerk global gesendete und empfangene Bytes, UDP und TCP getrennt
- Web-Privacy-Statistik und Zahl abgeblockter Bilder (keine aktiven Inhalte)
- Web Grafik in Bytes und eingesparte Zeit (LAN-Geschwindigkeiten nicht unterstützt)
- Zahl der durch den Firewall erlaubten oder abgeblockten TCP-Pakete
- Zahl der durch den Firewall erlaubten oder abgeblockten UDP-Pakete
- Summenzähler erlaubt/blockiert für aktive Firewall-Regeln
- Summenzähler gesendet/empfangen der aktiven Netzwerkverbindungen
- 60 Sekunden Echtzeitdarstellung aktiver HTTP- und sonstiger Netzwerkverbindungen

Die Auswahl, welche Gruppe in der Darstellung enthalten sein soll, kann im Menü „View – Options“ durch Anklicken entsprechender Auswahlkästchen getroffen werden.

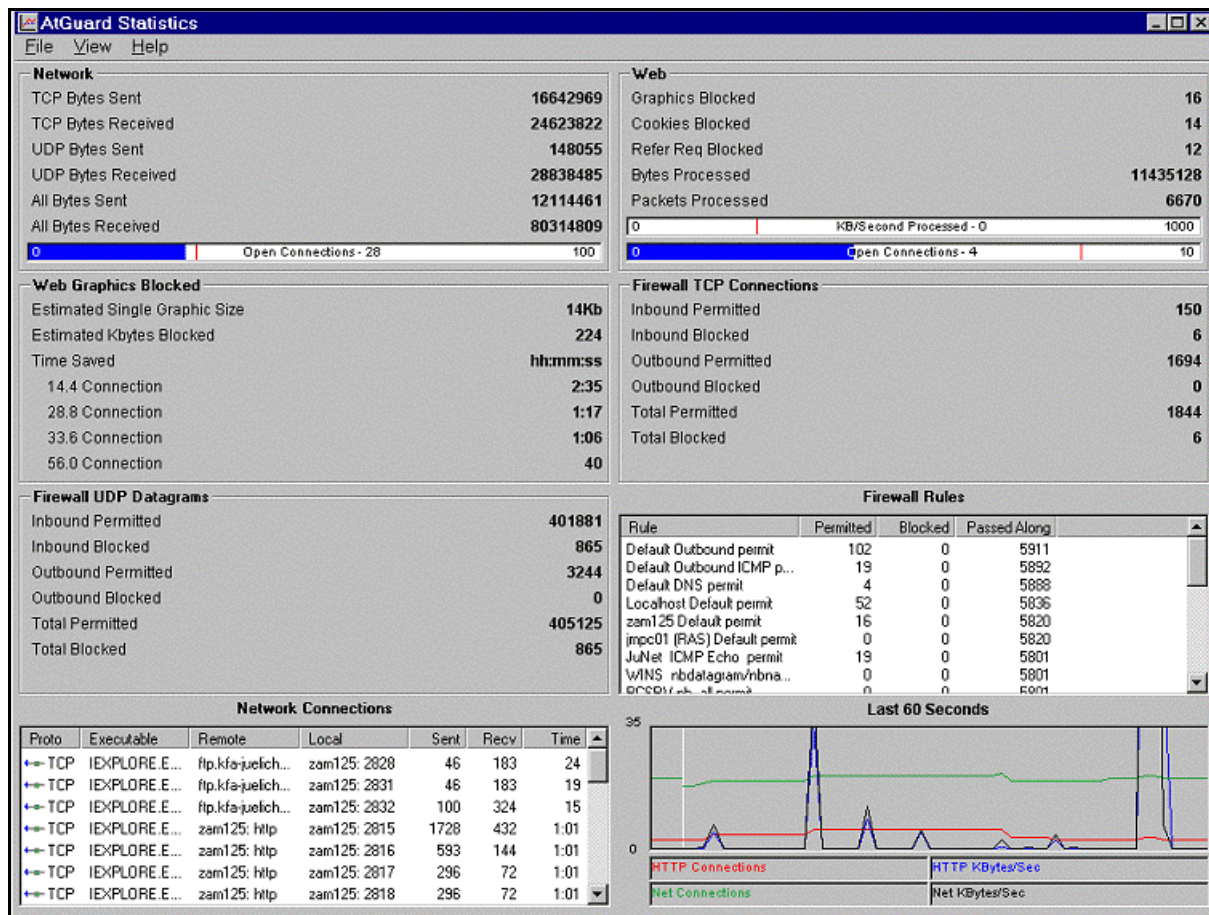


Abbildung 33: Die Anzeige der Web- und Verbindungsstatistik

Für einen groben Überblick oder eine schnelle Beurteilung der Aktivitäten des Webbrowsers mag diese Verkehrsstatistik gelegentlich von Nutzen sein, für eine detaillierte Überprüfung vor allem der Sicherheitseinstellungen ist das Eventlog sicherlich besser geeignet.

6 Der praktische Einsatz als Firewall im JuNet

6.1 Grundsätzliches zur PC-Sicherheit

JuNet, das campusweite Rechnernetz für die technisch-wissenschaftliche Datenkommunikation, ist ein für Forschungseinrichtungen oder Universitäten typisches, heterogenes, im wesentlichen aber IP-basierendes Netz. Da inzwischen auch PCs mit den neueren Windows-Betriebssystemen alle wichtigen Kommunikationsdienste über IP abwickeln können, decken die IP-Protokolle und darauf ausgerichtete Werkzeuge wie AtGuard de facto alle regulären Bedürfnisse ab. Selbstverständlich existieren in einem Umfeld wie dem Forschungszentrum auch viele Spezialsysteme wie Steuerungen oder Meßgeräte, die andere, oft proprietäre Protokolle benutzen. Diese unterstützen aber dann entweder die IP-Protokolle nicht und sind deshalb aus dem Internet heraus auch nicht angreifbar, oder sie verfügen über eigene, zusätzliche Sicherheitsmechanismen wie statische Routes, Access-Listen oder Verschlüsselung. Hinzu kommt, daß andere Protokolle als die IP-Protokolle vom JuNet-Backbone nicht transportiert werden.

In den folgenden Kapiteln sollen einige exemplarische Szenarien skizziert werden, wie PCs im JuNet eingesetzt und deren Sicherheit gegen IP-basierte Attacken durch einen Satz Regeln in AtGuard deutlich erhöht werden kann. Es sei allerdings auch deutlich darauf hingewiesen,

daß dies bei hohen Sicherheitsanforderungen (Personal- und personenbezogene Daten, Patent- und Vertragsdaten etc.) kein Ersatz für eine vollständige, starke Verschlüsselung aller Daten auf den Endsystemen selbst und der Datenkommunikation zwischen diesen Systemen („virtual private networks“) sein kann.

Die am einfachsten zu realisierende Firewallkonfiguration ist sicher diejenige, die freien Zugang vom und zum Internet erlaubt, um sich völlig ungehindert, damit aber auch weitgehend ungeschützt im weltweiten Inter- wie im firmeninternen Intranet^{*)} bewegen zu können. Einige wenige wohlbekanntere, als reguläre Anwendung kaum in Frage kommenden Applikationen sollte man dennoch ohne Einschränkung der Bewegungsfreiheit verhindern. Welche Anwendungen dies sind, ist letztlich der Entscheidung des einzelnen Benutzers überlassen. Vor allem gehören hierzu die bekannten Werkzeuge zur Fernsteuerung von PCs über das Netz, die gerne von Hackern zum Ausspähen fremder Systemen mißbraucht werden, wenn sie dort erst einmal durch eine Unvorsichtigkeit des Benutzers wie etwa durch Einspielen von Software aus unbekannter Quelle oder das Öffnen von Mail-Attachments dubioser Herkunft installiert wurden. Besonders unerfreulich sind diese Werkzeuge durch die Tatsache, daß selbst einzelne Tastenanschläge mitprotokolliert werden können, so daß auch bei Verwendung von Verschlüsselungssystemen die eingetippte „Passphrase“ ausgespäht werden kann. Das bekannteste Beispiel für solche Anwendungen ist BackOrifice, das sogar eine Videokopie des kompletten Benutzerbildschirms über das Netz versenden kann.

Neben der zitierten „Unvorsichtigkeit“ des Benutzers, zu der auch noch die Verwendung trivialer oder anonymer Paßwörter, Nichtbenutzung von Bildschirmschonern oder Fehler in der Systemkonfiguration zählen, existieren noch weitere Schwachstellen, die eine Installation solcher Software auch von außerhalb erlauben: Es sind dies einerseits Implementierungsfehler in der Systemsoftware selbst wie etwa bei der Java-Sandbox oder den FrontPage-Extensions, oder aber die ungehinderte Freischaltung aktiver Webinhalte wie Active Scripting oder ActiveX mit ungehindertem Download von Komponenten. Hier bietet bereits der Internet-Explorer selbst entsprechende Einstellmöglichkeiten, die unabhängig von den Einstellungen der Webfilter in AtGuard genutzt werden können und sollten.

Zwei Vorgehensweisen bieten sich zum Erstellen einer „maßgeschneiderten“ Sicherheitskonfiguration an:

1. Alles erlauben, die bekannten und nicht erwünschten Dienste aber verhindern
2. Nichts erlauben, die benötigten Dienste nach und nach zulassen.

Die erstgenannte Methode ist einfach und schnell anzuwenden, bietet jedoch keine Sicherheit vor unbekanntem Risiken. Die zweite Methode, die wesentlich höhere Sicherheit bietet, ist vor allem im Anfangsstadium sehr zeitraubend, solange kein erprobter Regelsatz vorliegt, sondern dieser erst mit Hilfe des Regelassistenten interaktiv erstellt werden muß. Es bietet sich an, diesen auf einem einzelnen PC zunächst über mehrere Tage zu erstellen und zu testen, um ihn dann auf weitere PCs mit annähernd gleichem Kommunikationsumfeld zu duplizieren.

Die in den folgenden Beispielen dargestellten Konfigurationen beziehen sich auf einen „stand-alone“-PC mit dem hypothetischen Internetnamen „myclient“, bei dem alle Benutzer- und Systemdaten auf der lokalen Festplatte liegen und dort durch den Systemadministrator jederzeit verändert werden können. Vorsicht ist geboten, wenn man in einer Clusterumgebung arbeitet, bei der wichtige Teile der Gesamtkonfiguration nicht auf der Klientenmaschine, son-

^{*)} Unter Intranet wird im folgenden JuNet, d.h. das gesamte IP-Netz des Forschungszentrums Jülich (134.94.0.0/255.255.0.0) verstanden. Der Internet-Explorer versteht darunter abweichend nur denjenigen Teil des Netzes, der über die eigene IP-Domäne des PCs, also beispielsweise „zam.kfa-juelich.de“, adressiert wird!

dern auf dem Server (im folgenden Beispiel mit Namen „myserver“) liegen. Das Aktivieren der Firewallfilter ohne vorherige Konfiguration einer Regel für den Serverzugang kann zu einer Situation führen, bei der man sich nicht mehr als Benutzer ins eigene System einwählen kann, um die fehlerhafte Einstellung zu korrigieren.

6.2 Der „offene PC“ mit minimalem Schutz

Dieser Abschnitt beschreibt eine Konfiguration nach der obengenannten Methode 1, bei der einige kritische Anwendungen zunächst durch spezifische Regeln abgeblockt, alle übrigen Kommunikationsarten aber freizügig in beiden Richtungen „Inbound“ und „Outbound“ zugelassen werden.

Man beginnt folglich die Regelerstellung mit den Regeln für die zu blockierenden Applikationen und ergänzt zum Schluß (in der Liste unten) eine gemeinsame Regel für den allgemeinen Datenverkehr in beiden Richtungen „Either“. Soweit im Regelnamen nicht explizit aufgeführt, werden dabei als Default „All Applications“, „All Services“, „Any Address“ ohne Zeitbeschränkung und ohne Logging angenommen. Verbindungsversuche zu Applikationen, die man unter allen Umständen unterbinden möchte, sollten unbedingt im Ereignislog für die Firewallregeln notiert werden, um gegebenenfalls eine Rückverfolgung der Quelle zu ermöglichen.

Der naheliegenden Versuchung, alle bekannten, aber vielleicht nicht erwünschten „Inbound“-Dienste wie RSH oder HTTP auf diese Art abzuriegeln, sollte man allerdings nicht erliegen: Auch das eigene Betriebssystem kann diese Dienste lokal über die eigene Internetadresse oder die Adresse des „localhost“ benutzen (siehe nächstes Kapitel).

Ein erster Satz Regeln für die offene Kommunikation würde also wie folgt aussehen:

Tabelle 1: Regeln für die offene Kommunikation

| Pos | Name | Action | Dir | Protocol | Application | Service remote/local | Address remote/local |
|-----|----------------------------------|--------|--------|------------|-------------|---|----------------------|
| 1 | Inbound Block Back Orifice / log | Block | In | TCP or UDP | Any | Any / Back-Orifice Back-Orifice-2000 | Any / Any |
| 2 | Inbound Block NetBus / log | Block | In | TCP or UDP | Any | Any / NetBus NetBus-Pro | Any / Any |
| 3 | Inbound Block PC-Anywhere / log | Block | In | TCP or UDP | Any | Any / PC-Anywhere-data PC-Anywhere-status | Any / Any |
| 4 | Default ICMP Permit | Permit | Either | ICMP | - | Any Type | Any / Any |
| 5 | Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | Any / Any |

Eine solche Konfiguration schützt neben dem unabhängigen Schutz vor aktiven Webinhalten durch die Webfilter nur vor drei besonders risikoreichen Applikationen und ist deshalb in einem Netz wie JuNet, wo die offene und schnelle Datenkommunikation wie in jedem Forschungs- oder Universitätsnetz im allgemeinen Vorrang vor Sicherheit genießt, weniger zu empfehlen.

6.3 Der „Intranet-PC“ für die freie Kommunikation im JuNet

Ein anderes, für die Arbeit in einem Intranet typisches Szenario liegt vor, wenn der PC zwar völlig freizügig innerhalb des firmeneigenen Netzes – in unserem Falle JuNet – kommunizieren soll, aber keinerlei Verbindung nach außerhalb gewünscht oder benötigt wird. Dies bietet Sicherheit gegenüber Attacken aus dem Internet, nicht aber gegenüber Attacken von möglicherweise im eigenen Intranet bereits durch Hacker übernommenen Rechnern oder gegen solche der eigenen „Kollegen“. Immerhin zeigt die Erfahrung im JuNet, daß mit Abstand die größere Gefahr tatsächlich aus dem weltweiten Internet droht, so daß mit der hier beschriebenen Einstellung schon ein beträchtliches Maß an Sicherheit hinzugewonnen wird. Da JuNet ein Klasse-B-Netz ist, wird für die interne Kommunikation die Netzadresse „134.94.0.0“ mit der Subnetzmaske „255.255.0.0“ eingetragen (nicht etwa die Subnetzmaske des eigenen Rechners!).

Um auch die Erreichbarkeit der eigenen Maschine und weiterer Rechner im Netz mit „Ping“ überprüfen zu können, und um die gelegentlich notwendige ICMP-Kommunikation mit dem IP-Gateway im eigenen Subnetz nicht zu behindern, sollte noch eine zusätzliche Regel „JuNet ICMP Default Permit“ für den freien ICMP-Verkehr innerhalb des JuNet eingetragen werden.

Auch die lokale Kommunikation des eigenen Systems mit sich selbst wird, soweit sie über die eigene IP-Adresse für „myclient“ abgehandelt wird, durch die Regeln für JuNet erfaßt und ist damit erlaubt. Das gilt jedoch nicht für die interne Systemkommunikation über die Adresse „localhost“ (= 127.0.0.1), die meist für solche Zwecke benutzt wird, und die nicht Bestandteil von JuNet ist. Daher muß auch für „localhost“ eine eigene Regel eingetragen werden, um lokale Client-Server-Applikationen, wie sie das Betriebssystem selbst verwendet, nicht zu behindern:

Tabelle 2: Regeln für die freie Kommunikation im JuNet

| Pos | Name | Action | Dir | Protocol | Application | Service remote / local | Address remote / local |
|-----|----------------------------------|--------|--------|------------|-------------|---|---------------------------------|
| 1 | Localhost Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | localhost / Any |
| 2 | JuNet ICMP Default Permit | Permit | Either | ICMP | - | Any Type | Any / Any |
| 3 | Inbound Block Back Orifice / log | Block | In | TCP or UDP | Any | Any / Back-Orifice Back-Orifice-2000 | Any / Any |
| 4 | Inbound Block NetBus / log | Block | In | TCP or UDP | Any | Any / NetBus NetBus-Pro | Any / Any |
| 5 | Inbound Block PC-Anywhere / log | Block | In | TCP or UDP | Any | Any / PC-Anywhere-data PC-Anywhere-status | Any / Any |
| 6 | JuNet Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | 134.94.0.0 / Any 255.255.0.0 |

Da dies eine sehr spezifische Regel darstellt, die nicht die Wirksamkeit der allgemeineren Regeln für JuNet „überschreibt“, kann sie ebenso wie die ICMP-Regel sinnvollerweise an den Anfang der Liste gestellt werden. Damit wird vermieden, daß der systeminterne Verbindungsaufbau über „localhost“ unnötigerweise durch Überprüfen weiterer Regeln, die ohnehin nie zutreffen, verlangsamt wird.

Möchte man trotz der offenen Kommunikation innerhalb des JuNet doch gerne wissen, wer beispielsweise (versehentlich oder gewollt) versucht, NETBIOS-Dienste auf dem PC anzu-

sprechen (Browsing, Shares), so kann man dies durch Eintrag einer zusätzlichen Regel mit „Ignore“ und eingeschaltetem Logging erreichen, auch ohne es explizit zu verhindern:

Table 3: Logging von NETBIOS-Zugriffen

| | | | | | | | |
|---|-----------------------------|--------|----|------------|-----|--------------------------------------|-----------|
| 6 | Default NETBIOS Ignore /log | Ignore | In | TCP or UDP | Any | Any / nbname, nbdatagram, nbssession | Any / Any |
|---|-----------------------------|--------|----|------------|-----|--------------------------------------|-----------|

Mit einem Adreßeintrag „Any“ würden auch externe Zugriffe verzeichnet, mit einem Adreßeintrag für JuNet nur solche aus dem eigenen Netz. Im Menü „Settings“ des Firewalls hat dann diese Konfiguration für freie Intranet-Kommunikation in JuNet folgendes Aussehen:

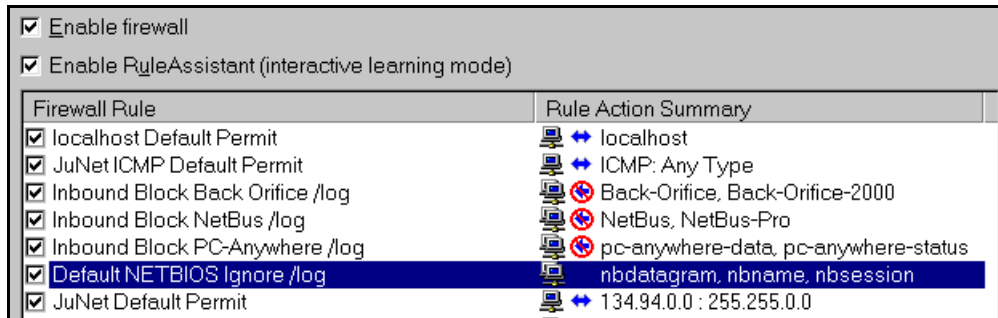


Abbildung 34: Die Regeln für freie Kommunikation im Intranet

Diese Regeln für die freie Kommunikation im JuNet können bei Bedarf jetzt noch durch Regeln ergänzt werden, die beispielsweise jedweden Verkehr zu einem bestimmten Host oder zu ganzen Teilnetzen des firmeneigenen Intranets verhindern oder aber Kommunikation zu einem einzelnen Host oder Netzwerk außerhalb des Adreßbereichs von JuNet zulassen. Als Beispiel sei ein hypothetisches Teilnetz **134.94.99.0** („hyponet“) mit bis zu 256 Rechnern, d.h. also mit der Netzmaske **255.255.255.0** angenommen, das gesperrt werden soll:

Table 4: Eine Einzelregel zum Sperren eines Teilnetzes

| | | | | | | |
|-----------------------|-------|--------|------------|-----|-----------|------------------------------------|
| Hyponet Default Block | Block | Either | TCP or UDP | Any | Any / Any | 134.94.99.0 / Any 255.255.255.0 |
|-----------------------|-------|--------|------------|-----|-----------|------------------------------------|

Diese Zusatzregel müßte, um wirksam zu sein, in der Liste sinngemäß vor der allgemeineren Regel 7 „JuNet Default Permit“ eingetragen werden.

6.4 Der „Normal-PC“ mit nutzungsspezifischer Konfiguration

Der sicher häufigste Anwendungsfall ist der eines einzelnen Stand-alone-PCs, der sich optimal gegen alle Risiken aus dem firmeninternen und aus fremden Netzen absichern, aber nicht innerhalb des gewohnten Umfeldes durch andauernd auf dem Desktop erscheinende Wizard-Fenster in seiner Arbeit behindert werden möchte. Das trifft besonders dann zu, wenn der Endanwender möglicherweise gar nicht die Kenntnisse besitzt, die durch den Regelassistenten gestellten Fragen qualifiziert zu beantworten. Typische PC-Anwendungen der letztgenannten Art sind PCs in Sekretariaten oder solche zur Unterstützung spezieller Geräte wie Drucker, NC-Steuerungen oder von Meßgeräten in Werkstätten und Labors. Aber auch auf den „JuNet-Normal-PC“, der vorwiegend im eigenen Subnetz oder in einer mehr oder weniger abgeschlossenen Rechnergruppe kommuniziert, treffen die folgenden Betrachtungen zu.

In diesem Fall führt kein Weg an einer individuellen Konfiguration der Filter vorbei, die je nach Anwendungsspektrum recht umfangreich (20 bis 30 Regeln) werden kann. Das setzt eine recht genaue Kenntnis des Kommunikationsumfeldes voraus, die entweder bereits vorhanden ist oder aber durch Einsatz des Regelassistenten im Laufe der Zeit gewonnen werden kann. Die praktische Erfahrung zeigt, daß eigentlich nur der zweite Ansatz Erfolg verspricht, da man sich sehr leicht in Art und Umfang der unterschiedlichen Kommunikationsdienste täuscht, mit denen man täglich bewußt oder unbewußt konfrontiert wird.

Das folgende Beispiel zeigt eine solche individuelle Konfiguration für einen PC namens „MYCLIENT“. Er kommuniziert mit verschiedenen Servern im JuNet wie Backup-, Time- oder FTP-Servern sowie zu allen Maschinen im eigenen Subnetz „MYNET“, das willkürlich als **134.94.77.0** mit einer Subnetmaske von **255.255.255.0** angenommen wird. Gleichzeitig möchte der Benutzer sich aber mit Ausnahme des eigenen Home-PCs „MYHOMEPC“ vor Zugriffen aus dem Telefon- bzw. ISDN-Netz (**Remote Access Service** des Forschungszentrums) und gegen einige weitverbreitete Dienstanforderungen wie **SNMP (Simple Network Management Protocol)** oder **Portmapper (Port 111 für Remote Shell, NIS, NFS)** schützen, ohne jedesmal interaktiv den Regelassistenten bedienen zu müssen. Zusätzlich sollen Verbindungsanforderungen des Rechners „BADHOST“ im eigenen Subnetz ebenfalls abgelehnt werden.

Die Liste der Filterregeln beginnt wie immer mit den Regeln 1 und 4 für die systeminterne Kommunikation über „localhost“ und die Kommunikation zur eigenen Adresse „MYCLIENT“. Die Regeln 2 für die Zeitsynchronisation der eigenen Systemuhr und 3 für die ständig benötigte IP-Namensauflösung (**Distributed Name Service**) wurde zur Vermeidung unnötiger Zeitverzögerungen in der Liste vorgezogen.

Tabelle 5: Individuelle Konfiguration eines typischen JuNet-PCs

| Pos | Name | Action | Dir | Protocol | Application | Service remote / local | Address remote / local |
|-----|---------------------------------|--------|--------|------------|-------------|------------------------------------|---------------------------------|
| 1 | LOCALHOST Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | localhost / Any |
| 2 | NTP Time Sync Permit | Permit | In | TCP or UDP | Any | Any / ntp time | ntp.kfa-juelich.de / Any |
| 3 | JuNet DNS Permit | Permit | Either | TCP or UDP | Any | domain / Any | 134.94.80.2-134.94.80.3 / Any |
| 4 | MYCLIENT Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | myclient / Any |
| 5 | MYHOMEPC (RAS) Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | myhomepc / Any |
| 6 | Default Outbound Permit | Permit | Out | TCP or UDP | Any | Any / Any | Any / Any |
| 7 | Default Outbound ICMP Permit | Permit | Out | ICMP | Any | Any Type | Any / Any |
| 8 | WINS nbdatagram / nbname Permit | Permit | In | TCP or UDP | Any | Any / nbdatagram nbname | wins.kfa-juelich.de / Any |
| 9 | PCSRV NETBIOS Permit | Permit | In | TCP or UDP | Any | Any / nbdatagram nbname nbssession | pcsrv.kfa-juelich.de / Any |
| 10 | ZELCDS NETBIOS Permit | Permit | In | TCP or UDP | Any | Any / nbdatagram nbname nbssession | zelcds.zel.kfa-juelich.de / Any |

| Pos | Name | Action | Dir | Protocol | Application | Service remote / local | Address remote / local |
|-----|--------------------------------------|--------|--------|------------|-------------|---|---|
| 11 | ADSMPCSRV Default Permit | Permit | In | TCP or UDP | Any | Any / Any | adsmpcsrv.zam.kfa-juelich.de / Any |
| 12 | FTP ftp-data Permit | Permit | In | TCP | Any | Any / ftp-data | ftp.kfa-juelich.de / Any |
| 13 | BADHOST Default Block / log | Block | In | TCP or UDP | Any | Any / Any | badhost / Any |
| 14 | MYNET ICMP Echo Permit | Permit | Either | ICMP | - | Echo Request Echo Reply | mynet / Any |
| 15 | MYNET nbdata/nbname Permit | Permit | In | TCP or UDP | Any | Any / nbdatagram nbname | mynet / Any |
| 16 | MYNET nbsession Permit /log | Permit | In | TCP or UDP | Any | Any / nbssessions | mynet / Any |
| 17 | MYNET HTTP Permit | Permit | In | TCP | Any | Any / http | mynet / Any |
| 18 | MYNET FTP Permit | Permit | In | TCP | Any | Any / ftp | mynet / Any |
| 19 | Back Orifice Inbound Block / log | Block | In | TCP or UDP | Any | Any / Back-Orifice Back-Orifice-2000 | Any / Any |
| 20 | NetBus Inbound Block / log | Block | In | TCP or UDP | Any | Any / NetBus NetBus-Pro | Any / Any |
| 21 | PC-Anywhere Inbound Block / log | Block | In | TCP or UDP | Any | Any / PC-Anywhere-data PC-Anywhere- status | Any / Any |
| 22 | Default dcom (135) Block | Block | In | TCP or UDP | Any | Any / dcom | Any / Any |
| 23 | Default portmap (111) Block | Block | In | TCP or UDP | Any | Any / portmap | Any / Any |
| 24 | JuNet-RAS1 Default Block / log | Block | In | TCP or UDP | Any | Any / Any | 134.94.114.0 / Any 255.255.254.0 |
| 25 | JuNet-RAS2 Default Block /log | Block | In | TCP or UDP | Any | Any / Any | 134.94.112.0 / Any 255.255.255.0 |
| 26 | ICMP Router Advertisement Block /log | Block | In | ICMP | - | Any / Router Advertisement | Any / Any |
| 27 | Default SNMP (161) Block /log | Block | In | TCP or UDP | Any | Any / snmp | Any / Any |
| 28 | MULTICAST Default Block | Block | In | TCP or UDP | Any | Any / Any | 224.0.0.0 – 239.255.255.255 / Any |

Als Kommunikationsrichtung wurde für die Regeln 1 und 3 bis 5 „Either“ eingetragen, obgleich weiter unten ohnehin die „Outbound“-Kommunikation generell zugelassen wird. Damit ist dies zwar äquivalent zu „Inbound“, ist aber vom praktischen Vorgehen her eher zu empfehlen, da es nicht zu logischen Fehlern bei einer späterer Einschränkung des Outbound-Verkehrs führt.

Regel 5 berücksichtigt den Kommunikationswunsch zu einem über das RAS-Netz des Forschungszentrums mit Modem oder ISDN angeschlossenen Heim-PC „MYHOMEPC“. Die Kommunikation zu allen anderen RAS-Zugängen ist durch die Regeln 24 und 25 unterbun-

den. Diese Regeln setzen allerdings eine feste Adreßzuordnung des PCs bei Einwahl über die Modemstrecken voraus (keine dynamische Adreßvergabe).

Die folgenden Regeln 6 und 7 gehen davon aus, daß alle Verbindungsanforderungen vom lokalen PC zu einem Rechner außerhalb, also die Richtung „Outbound“, vom Benutzer initiiert und daher gewollt sind. Diese Annahme ist solange gerechtfertigt, als der Rechner nicht bereits durch unerwünschte Fremdprogramme „infiziert“ ist, die ihrerseits vielleicht versuchen, Outbound-Verbindung zum Server eines Hackers oder zu weiteren „Hack-Kandidaten“ im Netz aufzunehmen. Die Einhaltung der üblichen Vorsichtsmaßnahmen (siehe oben) und eine regelmäßige Anwendung moderner Virensuchprogramme kann dazu beitragen, dieses Risiko zu vermindern. Aus diesem Grunde ist es gerechtfertigt, die Kommunikation nach außen, d.h. „Outbound“ generell zuzulassen oder wie oben auf JuNet zu beschränken.

Es folgen Regeln 8 bis 12, die für die PC-Kommunikation im JuNet die notwendige Konnektivität zu bestimmten Servern herstellen:

8. WINS-Server für die Windows-Namensauflösung IP/NETBIOS
9. Zugriff auf den PC-Distributionsserver PCSRV des ZAM über Windows-Shares
10. Zugriff auf den PC-Distributionsserver ZELCDS im ZEL über Windows-Shares
11. ADSM-Server für PC-Backups über das Netz im ZAM
12. Zugriff des FTP-Servers des Forschungszentrums auf den FTP-Datenport des eigenen PCs für den Dateitransfer von diesem Server

Regeln 14 bis 18 stellen die Kommunikation im eigenen IP-Subnetz sicher, wobei die Sessionverbindungen zu lokalen Shares (d.h. der Zugriff aus dem eigenen Netz auf freigegebene Ressourcen des PCs) zusätzlich im Log festgehalten werden. Allerdings ist der Rechner „**BADHOST**“, obgleich im eigenen Subnetz, explizit durch Regel 13 von der Kommunikation zur eigenen Maschine ausgeschlossen.

Mit Regel 17 und Regel 18 werden Anfragen aus dem eigenen Subnetz an je einen Webserver (http-Protokoll) und einen FTP-Server (ftp-Protokoll), die beide auf dem PC aktiv sind, zugelassen. Wie in Kapitel 4.3.2 geschildert könnte hier bei mehreren installierten Servern auch noch die genaue Applikation, die diese Dienste vermittelt, spezifiziert werden.

Die nachfolgenden Regeln 19 bis 21 blockieren wie bereits oben beschrieben die drei wichtigsten Anwendungen zur Fernsteuerung von PCs, während die Regeln 22,23 und 26,27 einige durch fehlerkonfigurierte Unixsysteme häufiger auftretende Dienstanforderungen abblocken, ohne daß jedesmal das Menü des Regelassistenten aktiviert wird.

Die letzte Regel 28 schließlich „rettet“ den PC-Benutzer vor besonders in Anwesenheit von SGI-Grafikarbeitsplätzen im Netz verbreiteten IP-Multicasts, die gemäß Definition bestimmten Netzen **224.0.0.0** bis **239.255.255.255** zugeordnet sind.

Konfiguriert man seinen Firewall in etwa gemäß diesen Vorgaben, so erzielt man ein hohes Maß an Sicherheit vor Angriffen, die von außerhalb des eigenen Subnetzes „**MYNET**“ an den PC herangetragen werden, verbunden mit einer komfortablen Arbeitsweise im eigenen Netz.

Wem die Einschränkung der Kommunikation auf das eigene Subnetz noch nicht genügt, weil er sich mit seinem PC etwa zusammen mit organisationsfremden Rechner in einem großen Gemeinschaftsnetz befindet, kann die Regeln für „**MYNET**“ durch entsprechende Regeln für „**MYSERVER**“ ersetzen. Allerdings muß dann die Regelliste unter Umständen noch durch einige zusätzliche Regeln wie etwa zur Nutzung eines Print- oder Mailservers ergänzt werden,

die sich normalerweise in einem lokalen Subnetz befinden und im obigen Beispiel durch die Regeln für „MYNET“ mit abgedeckt werden.

Wird auch die allgemeine Regel 6 für den Outbound-Verkehr eingeschränkt, so müssen weitere Regeln wie etwa für den Zugriff auf die Nameserver (Dienst „domain“, 134.94.80.2 und 134.94.80.3), Mailserver (Dienste „imap“ zu imapsrv.fz-juelich.de, „smtp“ zu mailrelay.fz-juelich.de) oder Webserver (Dienst „http“ zu www.fz-juelich.de) des Forschungszentrums eingetragen werden.

Hat man einmal eine solche doch recht aufwendige Konfiguration erarbeitet, so möchte man sie gerne mit kleineren Modifikationen wie etwa dem Namen des Zielrechners auch auf andere Systeme der gleichen Arbeitsgruppe exportieren. Leider wird diese Funktion derzeit durch AtGuard (noch) nicht unterstützt. Erfreulicherweise sind aber alle Einträge der Firewall-Konfiguration in der Windows-Registry im Zweig

[HKEY_LOCAL_MACHINE\SOFTWARE\WRQ]

gespeichert und lassen sich dort mit dem Registriereditor als Textdatei exportieren, modifizieren und auf dem Zielsystem wieder in die Registry importieren. Vor der Aktivierung des neuen Regelsatzes müssen selbstverständlich alle Rechner-spezifischen Parameter wie Namen und Internetadressen auf das neue Zielsystem und dessen Kommunikationsumfeld angepasst werden. Dies kann durch Editieren der *.reg-Datei oder nach dem Import mit Hilfe des Menüs „Settings“ erfolgen.

Zusammenfassend stellen sich dann die oben definierten Regeln in der Ansicht der AtGuard-Regelliste wie folgt dar:

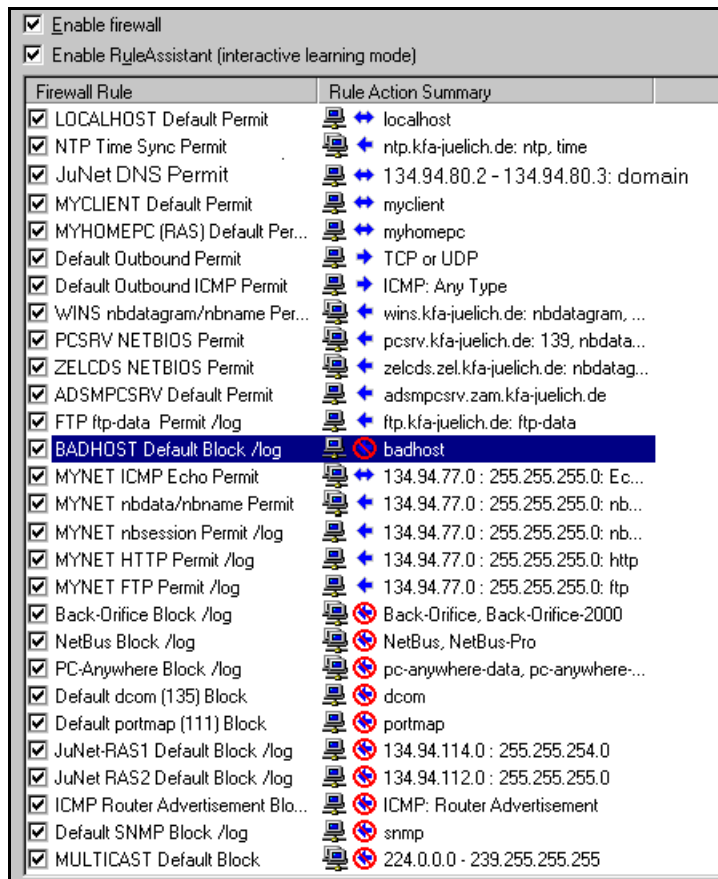


Abbildung 35: Regeln eines anwendungsspezifisch gesicherten „Normal-PCs“

6.5 Der „Spezial-PC“ mit minimalem Kommunikationsbedarf

Hier könnte es sich beispielsweise um einen PC handeln, der nur als Konsole zu einer bestimmten Server-Maschine benutzt wird und ansonsten keinerlei Außenkommunikation, auch nicht im firmenweiten Intranet, benötigt. Die IP-Namensauflösung kann dann über eine lokal gespeicherte Hosts-Datei (siehe Beispieldatei HOSTS.SAM auf dem Windows-Systempfad bzw. unter C:\WINNT\system32\drivers\etc\hosts.sam) erfolgen, so daß auch keine Kommunikation zu irgendwelchen Name- oder WINS-Servern erforderlich ist. Auf die Zeitsynchronisation kann verzichtet oder diese durch eine lokal angeschlossene Funkuhr bewerkstelligt werden.

Selbstverständlich wird auch hier vorausgesetzt, daß sowohl die eigene Maschine als auch der Server selbst als sicher und nicht infiziert anzusehen sind, da sonst auch jederzeit die Möglichkeit einer Manipulation der Firewallregeln bestünde. Allerdings wäre dies bei einer solch geschlossenen Konfiguration nur lokal oder vom eigenen Server aus möglich, da alle weitere Außenkommunikation ja durch die vorhandenen Regeln unterbunden ist.

Mit „myserver“ als Servernamen und „myclient“ als Name des eigenen PCs könnte dann eine solche Konfiguration unter den genannten Voraussetzungen wie folgt aussehen:

Table 6: Der Spezial-PC mit minimalem Kommunikationsbedarf

| Pos | Name | Action | Dir | Protocol | Application | Service remote / local | Address remote / local |
|-----|------------------------------|--------|--------|------------|-------------|------------------------|------------------------|
| 1 | Localhost Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | localhost / Any |
| 2 | Myclient Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | myclient / Any |
| 3 | Myserver ICMP Default Permit | Permit | Either | ICMP | - | Any Type | myserver / Any |
| 5 | Myserver Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | myserver / Any |

Für eine solche Konfiguration empfiehlt es sich, den Regelassistenten abzuschalten, da sonst bei jedem der in umfangreicheren Netzen üblichen, wenn auch meist unsinnigen Verbindungsversuche das Fenster des Regelassistenten aktiviert würde und wieder von Hand geschlossen werden müßte.

6.6 Der „geschlossene PC“ ohne Außenkommunikation

Ähnlich einfach zu konfigurieren wie der „offene PC“ ist dessen Gegenteil, ein PC, der fast ausschließlich für lokale Arbeiten wie Text- oder Bildbearbeitung eingesetzt wird. Dieser benötigt hierfür keinerlei Kommunikation nach außen und bräuchte eigentlich auch nicht an ein Netzwerk angeschlossen zu sein. Dennoch ergibt sich erfahrungsgemäß auch hier ab und zu die Notwendigkeit, einmal eine Datei wie z.B. ein Software-Update aus dem Netz zu holen oder jemandem kurzfristig eine Bilddatei zuzusenden. Für diesen Fall ist eine Konfiguration denkbar, die normalerweise jede Außenkommunikation unterbindet, die aber bei (seltenem) Bedarf kurzfristig für einige Minuten einfach deaktiviert und anschließend wieder reaktiviert wird. Die Wahrscheinlichkeit einer erfolgreichen Kompromittierung des Systems in dieser kurzen Zeit ist minimal, da ja das System normalerweise mit aktivierten Filtern im Netz nicht sichtbar ist. Auch hier sollte die systeminterne Kommunikation mit „localhost“ und „myclient“ noch möglich sein, falls diese von Anwendungsprogrammen oder vom System selbst benötigt wird:

Tabelle 7: Der PC ohne Außenkommunikation

| Pos | Name | Action | Dir | Protocol | Appli- cation | Service remote / local | Address remote / local |
|-----|--------------------------|--------|--------|------------|------------------|---------------------------|---------------------------|
| 1 | Localhost Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | localhost / Any |
| 2 | Myclient Default Permit | Permit | Either | TCP or UDP | Any | Any / Any | myclient / Any |

Jede weitere Kommunikation wird durch den Default (alles blockieren, was nicht durch eine Regel erlaubt ist) unterbunden.

7 Ausblick

AtGuard wurde auf mehreren PCs in JuNet unter den Betriebssystemen Windows 95, 98 und NT-4.0 Workstation installiert und über mehrere Wochen im Produktionsbetrieb getestet. In dieser Zeit wurden durch Einsatz des Regelassistenten nicht nur die Konfigurationen den oftmals überraschenden praktischen Erfordernissen angepaßt, sondern es wurden auch viele Fehlversuche zum Verbindungsaufbau entdeckt, die auf falsche Systemkonfiguration von Rechnern im Netz oder tatsächlich auf (meist automatisierte) Verbindungsversuche, sogenannte „Scans“ von Hackern aus dem Internet hindeuteten.

Um die Funktionsweise der Webfilter (und auch der Internet Explorer-Einstellungen) am praktischen Beispiel testen zu können, wurde eine spezielle Webseite entwickelt, die neben Werbeinhalten auch alle sicherheitsrelevanten Techniken wie Active Scripting (JavaScript und VBscript), ActiveX, Plugins und Privacy-Einstellungen definiert zu überprüfen erlaubt. Dabei wurde festgestellt, daß nicht alle Einstellungsänderungen sofort übernommen werden. Ein Neustart von AtGuard oder erneutes Anmelden bei Windows kann helfen, man sollte jedoch, um ganz sicher zu gehen, für die endgültige Arbeitskonfiguration den Rechner einmal neu starten.

Es wurde keine Beeinträchtigung des Systemdurchsatzes bei der Datenübertragung im Netz festgestellt, da durch den Firewall nur der Verbindungsaufbau, nicht aber jedes Paket einer stehenden IP-Datenverbindung überprüft wird. Das bedeutet andererseits, daß der Firewall auch nicht vor einer möglichen Übernahme einer aktiven Verbindung durch „Raten“ der IP-Sequenznummer schützt. Hier – siehe oben – hilft nur eine vollständige Verschlüsselung des Datenstromes.

Die Funktionalität der Software läßt an manchen Stellen noch einige Wünsche offen. Hierzu zählen

1. Eine feinere Differenzierung der Einstellmöglichkeiten der Webfilter und der Anzeigen des Assistenten bei den aktiven Webinhalten (diese Funktionalität hat allerdings der Internet-Explorer in den Versionen ab 4.01 bereits eingebaut, so daß diese ergänzend zu den Einstellungen in AtGuard genutzt werden sollte).
2. Die Möglichkeit, für „Remote Host“ neben Adressbereichen und ganzen Netzen auch Listen einzelner, nicht zusammenhängender IP-Adressen einzutragen.
3. Die Funktion, Ereignisse über das standardisierte „syslog“-Protokoll zu einem zentralen Logserver hin zu loggen, um sie dort im Kontext mit Logeinträgen anderer Rechner korreliert auswerten zu können. Diese Funktion wäre besonders wichtig zur Erkennung von Scanversuchen durch Hacker („Intrusion Detection“).

4. Ein Export des gesamten Event-Logs als Textdatei und eine Volltext-Suchfunktion zum schnellen Auffinden bestimmter Einträge.
5. Eine Import- und Exportmöglichkeit aller Regeln und Webfilter in einfachem Textformat und vielleicht ein separater Regeleditor, mit dem ein Satz vorhandener Regeln durch Ändern weniger Einträge auf individuelle PCs angepaßt und wieder installiert werden kann.
6. Eine kontextsensitive Hilfe bei der Regelerstellung im Menü „Settings“, zumindest aber eine Liste der verfügbaren Namen der einzutragenden Dienste. Diese Liste der tatsächlich benutzten Namen sollte außerdem konsistent mit der Namensliste in der Dokumentation sein.

Hinzu kommt sicher der Wunsch, die sehr eng auf den einzelnen Privatkunden zugeschnittene Verkaufspolitik der Fa. WRQ bei diesem Produkt auf eine breitere Basis zu stellen, die einen problemlosen Support einer größeren Anzahl an Endbenutzern wie zum Beispiel im Forschungszentrum Jülich ermöglicht. Insbesondere die derzeitige Update-Politik mit vielen Einzel-Updates ist für eine zentrale Softwaredistribution ungeeignet und kann leicht den an sich wünschenswerten Einsatz des Produktes be- oder verhindern.

Insgesamt stellt AtGuard aber eine einfach anzuwendende und empfehlenswerte Lösung für Windows-PCs im Internet dar, die über keine weitergehenden lokalen oder durch die Netzinfrastruktur bereits implementierten Sicherheitsmechanismen verfügen und sowohl lokal als auch weltweit im Netz kommunizieren möchten. Im Verbund mit den bereits vom Betriebssystem bereitgestellten Sicherheitsmechanismen und einem bewußten Umgang mit den Risiken der Internet-Kommunikation kann AtGuard dazu beitragen, einen PC für Angriffe von außen – vor allem für solche, die ansonsten unbemerkt bleiben würden – recht unattraktiv und damit sicher zu machen. Auf jeden Fall hilft AtGuard, das eigene Kommunikationsumfeld besser kennen und verstehen zu lernen, und es schützt nicht nur vor fremden Angriffen, sondern macht diese auch deutlich sichtbar. Selbstverständlich ist auch hier nie auszuschließen, daß AtGuard selbst Fehler enthält, die von Hackern mißbraucht werden könnten

8 Anhang: AtGuard-interne Port- und Servicenamen

Liste der von AtGuard intern zusätzlich benutzten IP-Ports und Dienste-Bezeichnungen (entspricht nicht genau dem aktuelleren Stand der Software):

| Service | Portnummer | Beschreibung |
|--------------------|------------|--|
| http | 80 | HTTP |
| www | 80 | HTTP |
| www-http | 80 | HTTP |
| http-alt | 800 | HTTP |
| http-alt-1 | 8008 | HTTP |
| http-proxy | 8080 | Oftentimes used as HTTP proxy |
| http-proxy-1 | 8088 | Oftentimes used as HTTP proxy |
| http-mgmt | 280 | HTTP management |
| https | 443 | HTTP server |
| gss-http | 488 | HTTP misc |
| fmpro-http | 591 | HTTP misc |
| http-rpc-epmap | 593 | HTTP misc |
| bootps | 67 | Bootstrap Protocol Server |
| bootpc | 68 | Bootstrap Protocol Client |
| dcom | 135 | Microsoft RPC end point to end point mapping |
| ldap | 389 | Lightweight Directory Access Protocol |
| video | 458 | Connectix and Quick Time Streaming protocols |
| video-1 | 545 | Connectix and Quick Time Streaming protocols |
| rtsp | 554 | Real Time Stream Protocol |
| mountd | 709 | NFS mount daemon |
| pcnfsd | 721 | PC NFS Daemon |
| irc | 194 | Internet Relay Chat protocol |
| irc-serv | 529 | Internet Relay Chat protocol |
| ircs | 994 | Internet Relay Chat protocol |
| ircu | 6665 | Internet Relay Chat protocol |
| ircu-1 | 6666 | Internet Relay Chat protocol |
| ircu-2 | 6667 | Internet Relay Chat protocol |
| ircu-3 | 6668 | Internet Relay Chat protocol |
| ircu-4 | 6669 | Internet Relay Chat protocol |
| socks | 1080 | Socks |
| lotusnote | 1352 | Lotus |
| ms-sql-s | 1433 | Microsoft misc |
| ms_sql-m | 1434 | Microsoft misc |
| ms-sna-server | 1477 | Microsoft misc |
| ms-sna-base | 1478 | Microsoft misc |
| orasrv | 1525 | Oracle |
| Tdisrv | 1527 | Oracle |
| Coauthor | 1529 | Oracle |
| nsvt | 1537 | HP's NSVT native protocol |
| nsvt-stream | 1570 | HP's NSVT TCP stream mode |
| remote-winsoc | 1745 | Remote Winsoc Proxy |
| netshow | 1755 | Microsoft's NetShow |
| icq | 4000 | ICQ chat program |
| aol | 5190 | America Online |
| aol-1 | 5191 | America Online |
| aol-2 | 5192 | America Online |
| aol-3 | 5193 | America Online |
| aol-4 | 11523 | America Online |
| Back-Orifice | 31337 | Back Orifice |
| NetBus | 12345 | Netbus |
| NetBus-2 | 12346 | Netbus2 |
| pc-anywhere-data | 5631 | pcAnywhere data port |
| pc-anywhere-status | 5632 | pcAnywhere status port |

| | | |
|-----------|-------|-------------------------------------|
| xserver | 6000 | X Server |
| vdolive | 7000 | VDOLive Player |
| msbd | 7007 | Microsoft MSBD (related to NetShow) |
| realaudio | 7070 | Real Networks Real Audio |
| quake | 26000 | Quake server game |
| quake2 | 27910 | Quake2 server game |
| quake2-2 | 27911 | Quake2 server game |

Literaturverzeichnis

- [1] N. Luckhardt „Schutzbehauptung, Sicherheitssoftware für Windows-PCs“, Zeitschrift c't 3/99, Seite 146 (1999)
- [2] D. Flanagan „JavaScript, The Definitive Guide“, O'Reilly, ISBN 1-56592-392-8 (1998)
- [3] U. Thiemann und K.Löffelmann „Visual Basic 6.0, Das Handbuch“, Microsoft Press, ISBN 3-86063-137-3 (1999)
- [4] P. Monadjemi „Visual Basic 6 Kompendium“, Markt & Technik Verlag, ISBN 3-8272-5440-X (1999)
- [5] W. Doberenz „Java“, Carl Hanser Verlag, ISBN 3-446-18854-1 (1996)
- [6] AtGuard On-line Help, <http://www.atguard.com/help> , Frequently Asked Questions <http://www.atguard.com/faq.html> und Dokumentation <http://www.atguard.com/help/docs> (1999)
- [7] R. Niederberger, „Firewalls in Forschungsnetzen: Konzepte, Anspruch und Realisierbarkeit“, PIK 3/97, pp. 128-133, <http://www.kfa-juelich.de/zam/docs/autoren97/niederberger.html> (1997)
- [8] Deutsches Forschungsnetz DFN, 6. Workshop „Sicherheit in vernetzten Systemen“, Bericht Nr. 87 (1999)