Forschungszentrum Jülich

Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402
Informationszentrum, Tel. (02461) 61-6658

Technische Kurzinformation

FZJ-ZAM-TKI-0349
J.Meißburger
23.03.2000

@Guard: Ein Firewall für Internet-PCs

Erhöhte Sicherheit durch IP- und Webfilter für Windows-PCs

Inhaltsverzeichnis:

---

1. Einleitung

AtGuard ist, ähnlich wie der TCP-Wrapper für Unix-Systeme, ein preiswertes Werkzeug zur Überwachung und Steuerung der Zugriffe aus dem Netz auf einen ans Internet angeschlossenen PC unter Windows 95/98/NT. Hersteller ist die Fa. WRQ (Wick Hill), die das Produkt ausschließlich on-line über das Internet vertreibt. Für das Forschungszentrum hat das ZAM einige Lizenzen erworben, so daß die Software auf dem PC-Server "**zelcds**" zum Download durch die PC-Verantwortlichen unter \\zelcds\atguard angeboten werden kann.

Neben regelbasierten Filtermöglichkeiten auf der Basis von Internet-Adressen und -Applikationen (IP-Port und Anwendung) bietet AtGuard zusätzliche Filtermöglichkeiten für das Browsen im World Wide Web wie etwa Werbe-, Cookie- oder HTTP-Referer-Filter. Auch die Möglichkeit, die Ausführung aktiver Inhalte wie Scripting, Java, ActiveX und Popup-Fenster zu unterbinden, ist sicherheitstechnisch von hohem Interesse. Die Filtererstellung wird durch interaktive Assistenen erleichtert.

AtGuard unterstützt selbslernend den Aufbau eines nach den Bedürfnissen des Benutzers "maßgeschneiderten" Firewalls durch eine dialoggeführte Regelerstellung, die automatisch beim Versuch eines Verbindungsaufbaus aus dem Netz aktiviert werden kann. Solche Regeln können für die gerade aktive Anwendung, für bestimmte Kommunikationspartner und Ports oder generell systemweit gelten.

Neben einem "Dashboard", das die Netzwerk- und Filteraktivitäten von AtGuard im Stile einer Taskleiste "gedocked" oder als normales Fenster anzeigt, werden konfigurierbare Ereignis-Logs und anwendungsspezifische IP-Statistiken der Netzzugriffe erstellt.

Eine detaillierte Beschreibung der Funktionen von AtGuard und ausführliche Konfigurationshinweise für den Betrieb im JuNet sowie allgemeine Hinweise zur Sicherheit von Windows-PCs sind (auch als .pdf) unter http://www.fz-juelich.de/zam/net/security/meissbu zu finden.

Seite 1

2. Die Installation

2.1 Informationen zum Produkt

Der originale Installationskit, der früher direkt vom Server des Herstellers WRQ heruntergeladen werden konnte, steht nicht mehr zur Verfügung. Die zugrunde liegende AtGuard-Technologie wurde an die Firma Symantec verkauft, die diese möglicherweise in Zukunft als neues Produkt anbieten wird. Deshalb ist AtGuard derzeit im Handel nicht mehr erhältlich. Das ZAM hat jedoch für das Forschungszentrum noch eine größere Zahl von Lizenzen gekauft und stellt die letzte beim Hersteller verfügbare Version V3.22 auf dem ZEL-Server unter

\\zelcds\atguard

zum Download durch die berechtigten PC-Verantwortlichen zur Verfügung.

2.2 Installation vom Server "zelcds"

Den aktuellen Kit oder benötigte Updates von **\\zelcds\atguard** auf C:\Temp herunterladen. Das Readme.txt enthält noch einige aktuelle Hinweise zur Distribution und Installation. Die Versionen atgdxxx**u**.exe sind Updates und können nur ausgehend von ATGD310.EXE nacheinander installiert werden, ATGD322.EXE ist die aktuelle Version für eine Neuinstallation. Alle auf zelcds liegenden Softwarekits sind bereits lizenziert und dürfen nur für dienstliche Zwecke innerhalb des Forschungszentrums kopiert werden.

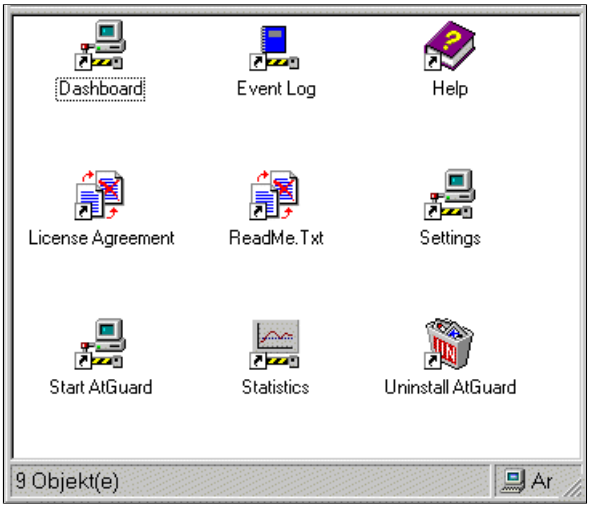
atgd3xx.exe ausführen

.. 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: Finish oder ggf. Einspielen des nächsten Updates.

Reboot

Nach dem Reboot steht AtGuard als Applikation allen Benutzern des PCs mit einer eigenen Programmgruppe,



einem Icon in der Taskleiste und einem am oberen Bildrand gedockten oder mit der Maus frei beweglichen "Dashboard"

zur Verfügung.

Seite 1

3. Die Funktionen

Die Funktionen der neu errichteten Programmgruppe "AtGuard" sind durch durch Doppelklicken der Icons der Programmgruppe, durch Klicken des Icons in der Taskleiste oder durch Öffnen eines Pulldown-Menüs im Dashboard unter verfügbar. Hier können auch die Einstellungen für den automatischen Start, für die Anzeige von Icon und/oder Dashboard sowie für den Paßwortschutz der Konfiguration vorgenommen werden.

3.1 Das "Dashboard"

Das zentrale Anzeige- und Steuerelement für AtGuard ist das Dashboard, in dem durch Anklicken der Auswahlkästchen die Funktionen

- Network Activity
- Web Network Activity
- Ads Blocking
- Privacy Protection
- Firewall Activity

unmittelbar ein- bzw. ausgeschaltet werden können. Die entsprechenden Einstellungen im Pulldown-Menü "Properties" erlauben die Anzeige dieser Funktionen einzeln an- und abzuschalten. Das Dashboard selbst kann mit "Hide Dashboard" weggeschaltet und über das Icon in der Taskleiste über "Dashboard" wieder sichtbar gemacht werden. Wird im Munüpunkt "Properties" die Funktion "Autohide" aktiviert, so ist das Dashboard nur sichtbar, solange die Maus am oberen Bildrand positioniert ist.

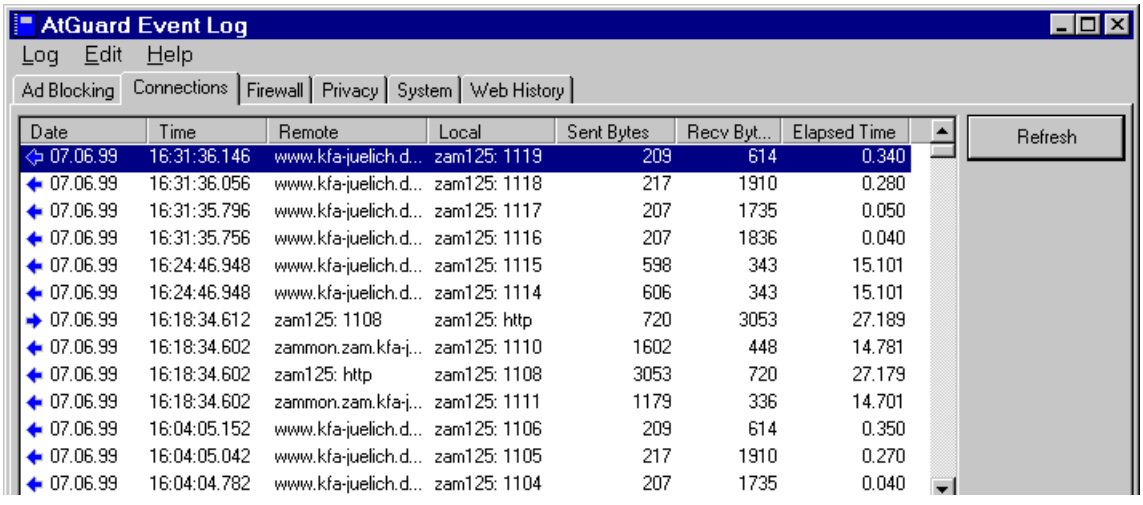
Das Dashboard zeigt mit den angezeigten Zählern die aktuelle Summenstatistik zu IP-Verbindungen, Web-Aktivität, Web-Filtern und Firewall-Filtern. Ein Klick auf die Zahl der offenen Netzwerkverbindungen (15) zeigt eine Liste der gerade aktiven IP-Verbindungen:

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: nbsession	0	0	1:40:01
TCP	war-ftpd.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-ftpd.exe	Listening		zam125: 1033	0	0	1:39:44
UDP	war-ftpd.exe	Listening		zam125: portmap	0	88	1:39:44

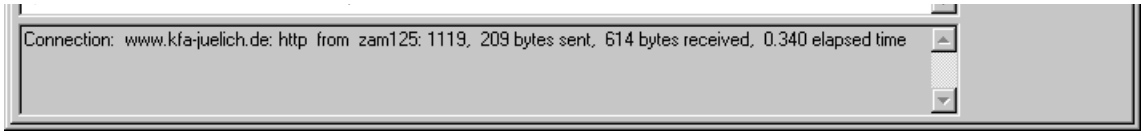
Seite 1

3.2 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:



Date	Time	Remote	Local	Sent Bytes	Recv Byt...	Elapsed Time
07.06.99	16:31:36.146	www.kfa-juelich.d...	zam125: 1119	209	614	0.340
07.06.99	16:31:36.056	www.kfa-juelich.d...	zam125: 1118	217	1910	0.280
07.06.99	16:31:35.796	www.kfa-juelich.d...	zam125: 1117	207	1735	0.050
07.06.99	16:31:35.756	www.kfa-juelich.d...	zam125: 1116	207	1836	0.040
07.06.99	16:24:46.948	www.kfa-juelich.d...	zam125: 1115	598	343	15.101
07.06.99	16:24:46.948	www.kfa-juelich.d...	zam125: 1114	606	343	15.101
07.06.99	16:18:34.612	zam125: 1108	zam125: http	720	3053	27.189
07.06.99	16:18:34.602	zammon.zam.kfa-j...	zam125: 1110	1602	448	14.781
07.06.99	16:18:34.602	zam125: http	zam125: 1108	3053	720	27.179
07.06.99	16:18:34.602	zammon.zam.kfa-j...	zam125: 1111	1179	336	14.701
07.06.99	16:04:05.152	www.kfa-juelich.d...	zam125: 1106	209	614	0.350
07.06.99	16:04:05.042	www.kfa-juelich.d...	zam125: 1105	217	1910	0.270
07.06.99	16:04:04.782	www.kfa-juelich.d...	zam125: 1104	207	1735	0.040



Das Pulldown-Menü "Log" bietet die nützlichen Zusatzfunktionen, Ereignis-Einträge als Textdateien abzuspeichern, sie auszudrucken, oder sie z.B. nach jeder Abmeldung vom System automatisch zu löschen.

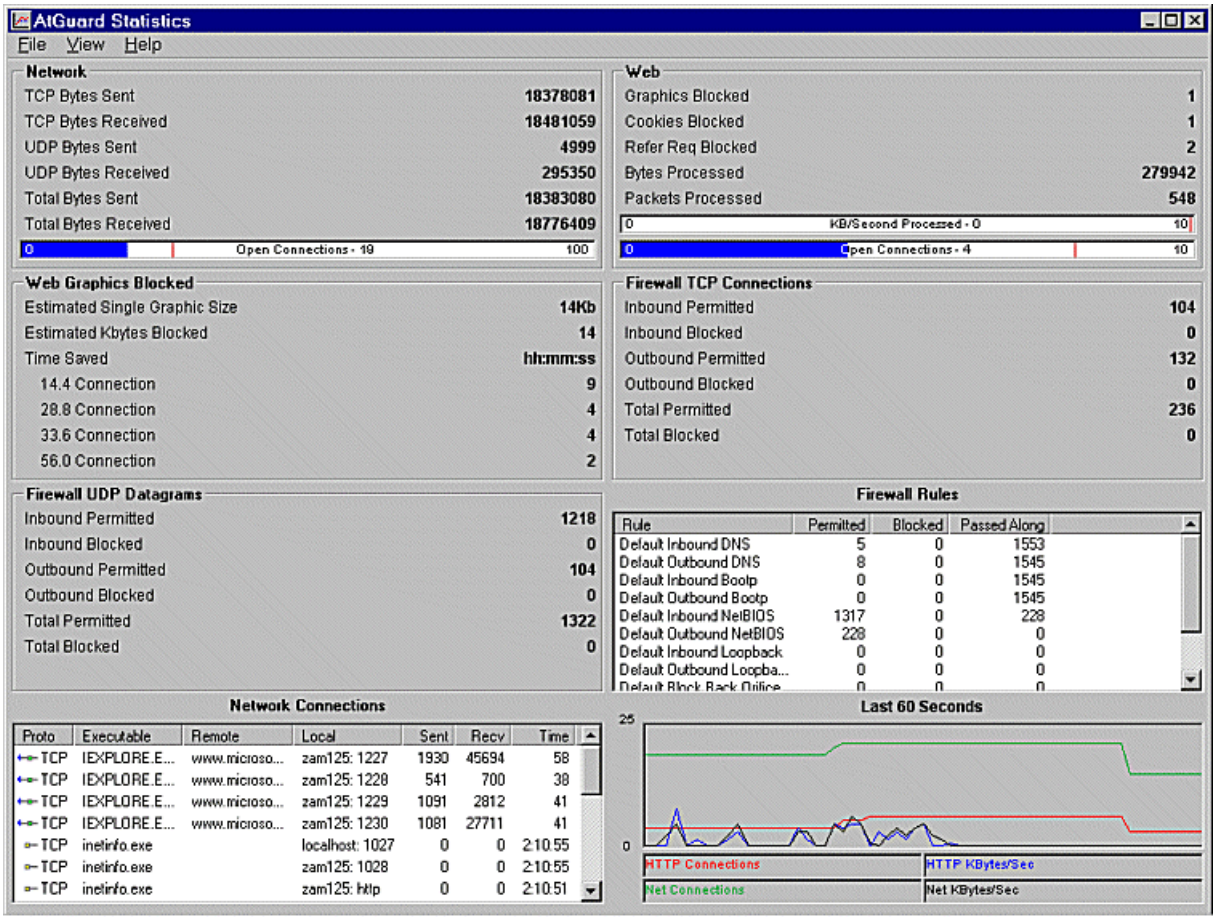
Seite 1

3.3 Die Statistik

Summen- und Verkehrsstatistiken werden nach den Gruppen

- Netzwerk global
- Web-Statistik
- Web Grafik
- Firewall TCP-Verbindungen
- Firewall UDP-Verbindungen
- Angesprochene Firewall-Regeln
- Netzwerk-Verbindungen
- 60 Sekunden Echtzeit

sortiert wie folgt angezeigt:



Eine Auswahl der anzuzeigenden Statistikgruppen kann über den Menüpunkt "View - Options..." getroffen werden.

Seite 1

3.4 Das Konfigurationsmenü "Settings..."

Alle sonstigen Einstellungen, insbesondere die Einstellungen zu den Webfilter- und Firewall-Funktionen und die Definition der Firewall-Regeln werden über das Konfigurationsmenü **"Settings..."** vorgenommen. Das Menü kann

- aus der Programmgruppe durch Klicken des Icons "Settings"
- "Settings..." im Pulldown-Menü des Dashboards
- oder mit der rechten Maustaste auf dem AtGuard-Symbol im Taskbar und "Settings..."

aufgerufen werden. Es hat drei Unterpunkte:

- **Options** zur Einstellung der Startup-Eigenschaften von AtGuard
- **Web** zur Definition der Filter für das Web-Browsing
- **Firewall** zur Definition des Verhaltens des IP-Firewalls (Regeldefinition)

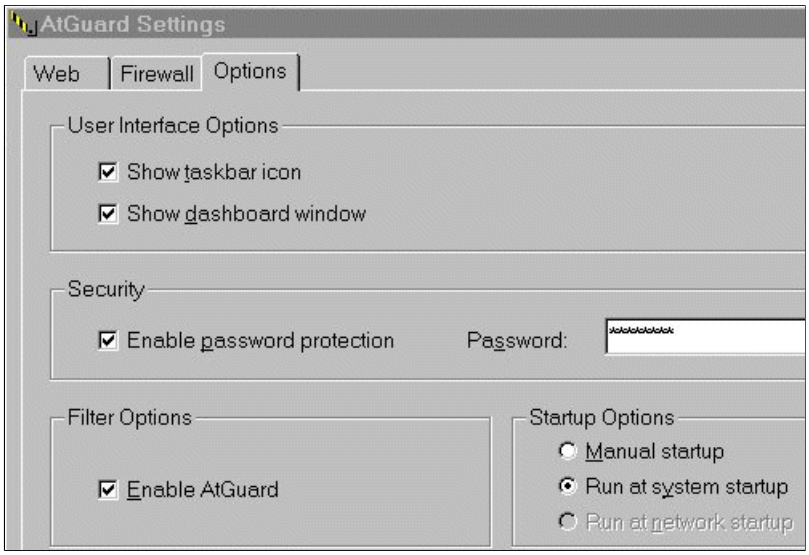
Diese Einstellungen werden an Hand eines typischen Beispiels für einen PC in JuNet im folgenden Kapitel erläutert.

Seite 1

4. Das Menü "Settings": Webfilter und Firewall

4.1 Options

Die Einstellungen für den Start von AtGuard werden im Untermenü "Options" festgelegt. Eine empfohlene Einstellung wäre wie folgt:



Damit startet AtGuard automatisch bei Systemstart mit aktivierten Anzeigen und Filterfunktionen. Die Konfiguration insbesondere des Firewalls ist durch ein Passwort gegen unbefugte Änderungen geschützt.

Will man in einer ersten Phase zunächst einen Überblick über die typischen Netzwerkaktivitäten des PCs gewinnen, so empfiehlt sich der Einsatz des weiter unten beschriebenen Regel-Assistenten für den

Firewall. In diesem Fall sollte man temporär den Paßwortschutz abschalten, da sonst wiederholt bei jedem neuen Verbindungstyp, für den der Assistent eine Regel erstellt, das Security-Paßwort eingegeben werden muß.

4.2 Webfilter

Im Untermenü "Web" werden die Einstellungen für das Filtern von Web-Inhalten festgelegt und durch Auswahl von "Enable web filters" aktiviert. Sinnvolle Default-Einstellungen sind beispielsweise (aufgeführt sind die aktivierten Funktionen):

4.2.1 Filters....

Ad Blocking: eingeschaltet
Privacy: eingeschaltet
Active Content: eingeschaltet

Cookie Assistant:
aus oder ein, je nachdem, ob man Cookies immer akzeptieren oder je nach Domain unterschiedlich behandeln oder ganz ablehnen möchte. Ist der Cookie-Assistant eingeschaltet, so erscheint bei jedem neuen Cookie, das ein Server ablegen möchte, das Popup-Fenster des "Cookie-Wizards". In diesem kann dann spezifiziert werden, wie mit diesem Cookie in Zukunft verfahren werden soll (Der Aufbau des Fensters entspricht dem unter 4.3.1 gezeigten Fenster des Regel-Assistenten). Empfehlung: Ausgeschaltet.

Java/ActiveX-Assistant:
Je nach Sicherheitsansprüchen aus oder ein, um z.B. Java und vor allem ActiveX-Inhalte nur von vertrauenswürdigen Servern zu laden und auszuführen. Empfehlung: Eingeschaltet.

HTTP Port List:
Hier können zusätzliche Portadressen z.B. für eigene, nicht dem Standard entsprechende Webserver eingetragen werden, für die dann Webinhalte ebenfalls gefiltert werden.

Mit "Add Site" können zusätzliche Webfilter für ganz bestimmte Websites (IP-Domains oder Hosts) in einer hierarchischen Liste abgelegt werden. Root dieser Liste ist stets "Default", d.h. die allgemein gültige Einstellung. Hierunter können Domains oder Websites und hierunter wieder einzelne Websites (Hosts) eingetragen werden, für die die Einstellungen der übergeordneten Hierarchiestufe jeweils übernommen bzw. überschrieben werden.

4.2.2 AdBlocking

Hier lassen sich mit "Add..." zusätzlich zu den bereits eingerichteten, typischen HTML-Tags und URL's, die auf Werbeinhalte verweisen, weitere HTML-Elemente, die nicht angezeigt werden sollen, eintragen.

Eine weitere Methode, beim Browsen von (häufig besuchten) Webinhalten unerwünschte Links (Bilder, Werbeinhalte etc.) interaktiv zu unterbinden besteht darin, mit der rechten Maustaste ein solches Link aus dem Browser in den Papierkorb des Dashboards zu kopieren. Nach einer kurzen Bestätigung des URLs wird dieses Link in die Liste der zu sperrenden Webinhalte übernommen.

4.2.3 Privacy

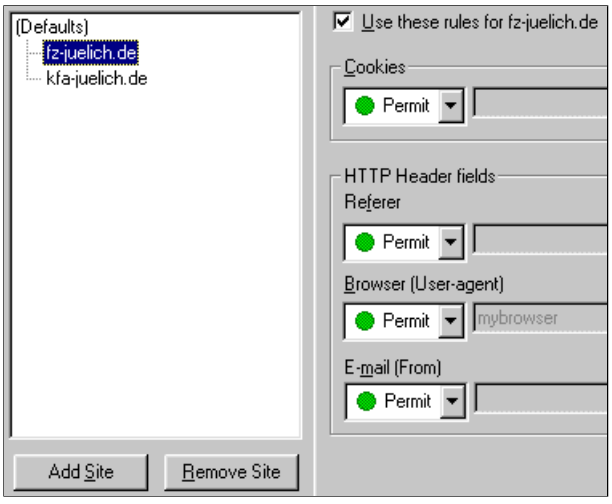
Hier wird festgelegt, welche Informationen der Browser an den Webserver oder an einen "third party"-Server weitergibt. Es sind jeweils drei Einstellungen wählbar:

1. Block: AtGuard ignoriert die Serveranfrage und schickt keine Information zurück
2. Permit: Die Anfrage wird wie üblich beantwortet
3. Reply: AtGuard beantwortet die Anfrage mit einem beliebig wählbaren Text (nicht empfehlenswert!)

Empfohlene Default-Einstellungen sind:

- Cookies: Permit
  Cookies werden häufig benutzt und sind unkritisch, liefern aber Informationen über das Verhalten des Benutzers im Web (Profil).
- Referer: Block
  Beim (durch einen besuchten Server veranlaßten) Besuch eines "third-party"-Servers muß die Information über den zuerst besuchten Server nicht weitergegeben werden - dies dient meist der Unterstützung von Werbe- und E-Commerce-Servern.
- Browser (User-agent): Permit
  Damit kann der Server den Typ und das Betriebssystem des Browsers abfragen.
  Positiv: Damit ist, falls vom Server unterstützt, eine optimale Ausnutzung der Fähigkeiten des lokalen Browsers gewährleistet.
  Negativ: Andererseits kann diese Information mißbraucht werden, um systemspezifischen "Hack"-Versuchen zustätzliche Informationen über das Betriebssystem zu liefern.
- E-mail: Block
  Damit wird unterbunden, daß der Browser die evtl. konfigurierte E-Mail-Adresse des lokalen Systems an einen Webserver weitergibt (Keine Informationen für "Spammer" !).

Mit "Add Site" können auch hier diese Regeln für JuNet-interne Kommunikation außer Kraft gesetzt werden, indem die beiden Domänen "fz-juelich.de" und "kfa-juelich.de" hinzugefügt werden. Durch Anklicken der Domänennamen und "Use these rules for kfa-juelich.de bzw. fz-juelich.de" können dann für die interne Kommunikation alle Einstellungen beispielsweise auf "Permit" geschaltet werden:



4.2.4 Active Content

Hier werden die Default-Einstellungen zur Behandlung von aktiven Inhalten (Java, JavaScript und ActiveX) festgelegt. Je nach besuchter Domain oder Site können diese mit Hilfe des bei Bedarf automatisch aktivierten Assistenten dann noch Site-spezifisch und interaktiv modifiziert werden.

Empfohlene Default-Einstellungen:

- Script: Block only popup window script
  Dies verhindert die oft lästigen, zusätzlichen Popup-Fenster, die von vielen Servern zu Werbezwecken benutzt werden. Wer (insbesondere fehlerhaftes) JavaScript vielleicht für bestimmte Webserver abschalten möchte, kann dies an dieser Stelle tun.
- Binary Executables: Block ActiveX controls
  Java Applets sind relativ sicher (actuelle Browserversionen vorausgesetzt). ActiveX-Applikationen sind riskanter und sollten als Default besser ausgeschaltet werden.
- Make animated images non-repeating
  Diese Einstellung ist eigentlich selbstverständlich und zur Reduktion unnötiger Netzlast für Webbrowsing über NT-Terminalserver oder X11-Windowterminals (z.B. WinCenter von NCD) unbedingt zu empfehlen !

Wichtiger Hinweis: Auch das Zulassen von Scripting stellt bereits ein erhöhtes Sicherheitsrisiko dar. Allerdings benutzt die Mehrzahl der Server derzeit Scripting, so daß ein Abschalten für eine flexible Navigation im Internet nicht praktikabel erscheint. Es sei hier auch ausdrücklich auf die ergänzenden Sicherheitseinstellungen der Browser selbst verwiesen.

Seite 1

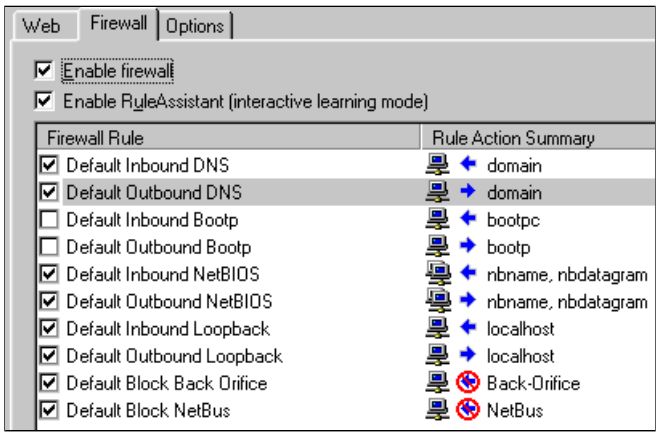
4.3 Firewall

Hier werden die Einstellungen und Regeln für den eingebauten Firewall abgelegt, die bei jeder Netzwerkverbindung sequentiell durchlaufen und überprüft werden. Je nach Ergebnis wird der Verbindungsversuch dann akzeptiert oder abgelehnt und in den Event-Logs registriert. Die Filterfunktion des Firewalls wird durch Auswahl der Checkbox "Firewall" im Dashboard oder durch "Settings - Enable firewall" im AtGuard Setup aktiviert.

4.3.1 Default-Regeln und interaktiver Lernmodus

Das Prinzip des Firewalls besteht darin, für jede IP-Verbindungsanforderung deren Charakteristika wie IP-Adresse, IP-Port (Service), Applikation und Uhrzeit an Hand einer Liste vordefinierter Regeln zu überprüfen und die Verbindungsanforderung je nach Ergebnis zuzulassen oder abzulehnen.

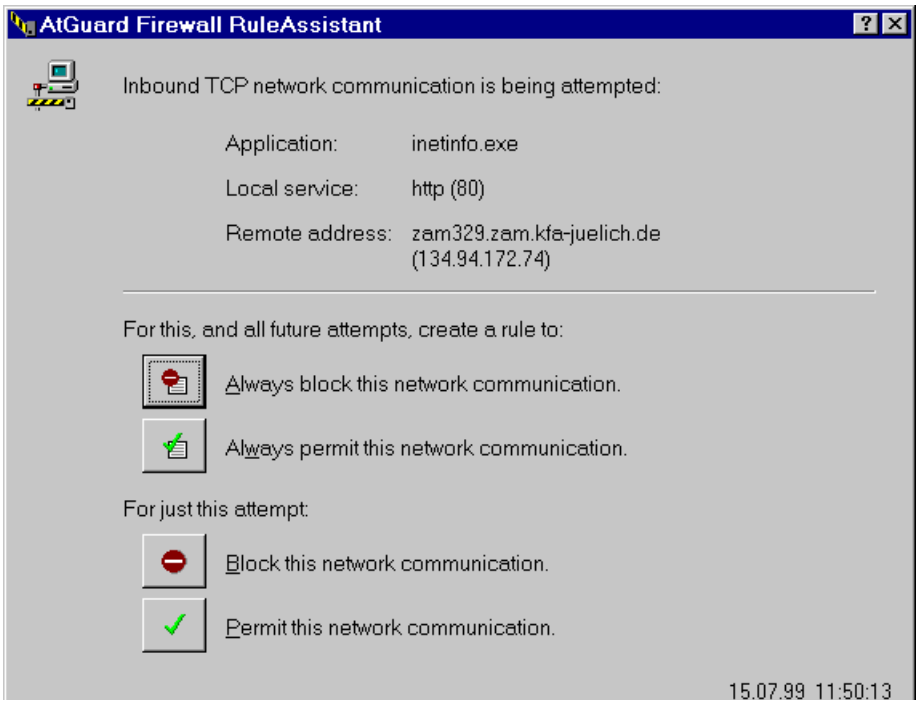
Bei eingeschaltetem Firewall werden die dort definierten Regeln **sequentiell von oben nach unten durchlaufen** und abgeprüft. Sobald eine "passende" Regel gefunden wird, wird diese angewandt und alle weiter unten definierten Regeln werden ignoriert. Ein Verbindungsversuch, für den keine passende Regel existiert, wird per Default abgelehnt und es wird, falls er eingeschaltet ist, der unten beschriebene "Rule-Assistant" des interaktiven Lernmodus aktiviert.



Die mitgelieferten Standardeinstellungen erlauben nur einige für die Internet-Kommunikation fast immer erforderlichen Standard-Dienste wie z.B. den Name-Service DNS und blockieren die kritischen Hacker-Attacken "Back-Orifice" und "NetBus". Für PCs in JuNet werden auch in- und outbound bootp üblicherweise nicht benötigt und können abgeschaltet werden. (Die zugehörige Regel wird damit außer Kraft gesetzt, aber nicht gelöscht, so daß sie jederzeit wieder reaktiviert werden kann).

Eine Besonderheit von AtGuard ist der interaktive Regel- Assistent, 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 erlaubt menügesteuert die Definition neuer Regeln, nach denen diese Verbindungsanfrage und alle weiteren Verbindungen dieses Typs behandelt werden sollen. Bei Bedarf werden die Eingaben dann als neue Firewall-Regel automatisch der Regelliste hinzugefügt.

Die oben gezeigten Default-Einstellungen erlauben keine "offene" IP-Kommunikation und sind vor allem dann sinnvoll, wenn man in kleinen Netzen oder nur dediziert mit ein, zwei Anwendungen auf einigen wohlbekannten Rechnern arbeiten möchte. Für diese wenigen Verbindungen werden dann die zusätzlich benötigten Regeln interaktiv mit dem Regel-Assistenten festgelegt. Die Default-Einstellungen können auch sinnvoll benutzt werden, wenn man einmal testweise einen Überblick über eigene (outbound) und fremde Verbindungsversuche (inbound) zum eigenen PC gewinnen möchte. Ein Verbindungsversuch zum Webserver des PCs wird dann vom Regel-Assistenten beispielsweise mit folgendem Fenster angezeigt:



Die Verbindung kann dann "For just this attempt" temporär akzeptiert oder abgelehnt werden, oder es kann menügeführt eine neue Regel für diesen Verbindungstyp aufgestellt und der Regelliste hinzugefügt werden.

4.3.2 Ein Beispiel: Regeln für die JuNet-interne Kommunikation

Mit "Add..." können von Hand zusätzliche Firewall-Regeln definiert werden. Es sei nochmals daran erinnert, daß alle Regeln von oben nach unten in der Liste abgearbeitet werden. Genügt also eine Verbindung einer der Regeln der Liste, werden keine weiteren Regeln für diese Verbindung mehr abgeprüft, der "erste Treffer" zählt !".

Um beispielsweise einen PC ohne jede Einschränkung im Netz des Forschungszentrums zu betreiben und gleichzeitig jeden Zugang von und nach draußen zu unterbinden, müssen vier weitere Regeln definiert und in der richtigen Reihenfolge an den Anfang der Liste gestellt werden. Als erstes werden die Regeln aufgeführt, die auf jeden Fall ein "permit" erhalten sollen: Das sind

1. Default Inbound Loopback und
2. Default Outbound Loopback

d.h. die Kommunikation des PCs mit sich selbst unter allen möglicherweise aktiven Serveradressen. (Solche Client/Serverkommunikation mit der eigenen "localhost"-Adresse kann u.U. innerhalb einer lokalen Applikation ablaufen).

Als nächstes in der Liste stehen die Regeln für zwei gefährliche "Hacker"-Anwendungen, "Back-Orifice" und "Netbus", die unter allen Umständen abgeblockt und im Eventlog erfaßt werden sollen (auch JuNet-intern !):

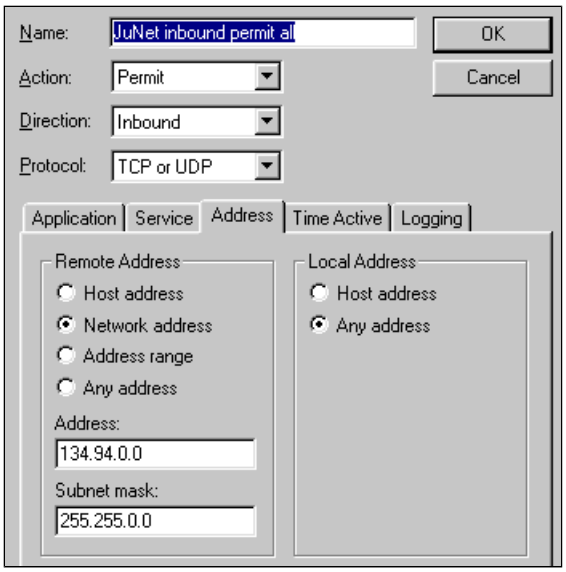
3. Default Block Back Orifice
4. Default Block NetBus

Danach folgen zwei Regeln, die Inbound- und Outbound-Verkehr zu jeder Adresse im JuNet ohne Einschränkung erlauben, sowie zwei weitere Regeln, die jede Kommunikation mit irgendeiner beliebigen Internetadresse verhindern:

5. JuNet inbound permit all
6. JuNet outbound permit all
7. Default inbound block
8. Default outbound block

Damit ist Kommunikation vom und zum lokalen PC nur noch innerhalb des Adreßbereiches von JuNet (134.94.*.*) möglich. Wer dies wünscht, kann im Untermenü "Logging" die Erfassung solcher Verbindungen im Eventlog aktivieren.

Regel 5 hat dann beispielsweise folgendes Aussehen:

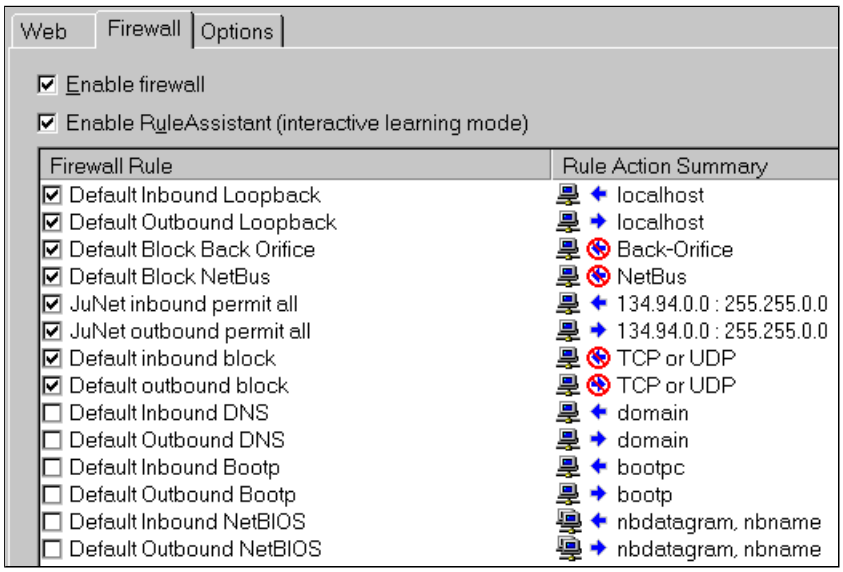


Sie erlaubt jedem Rechner im JuNet den Zugriff auf den eigenen PC zu jeder dort verfügbaren IP-Anwendung, und dies (Default) 24 Stunden täglich. Wer diesen Zeitraum einschränken oder die einzelnen Zugriffe im Ereignislog erfassen möchte, kann dies mit den Einstellungen unter "Time active" und "Logging" tun. Ebenso läßt sich der Zugriff mit "Service" auf bestimmte IP-Dienste (Ports) oder mit "Application" auf bestimmte Applikationen beschränken.

Regel 6 ist identisch mit der ersten, lediglich die Richtung der Datenpakete ist umgekehrt ("outbound" = vom lokalen PC zu einer Adresse im Netz, "inbound" = von außen zu einer Adresse des lokalen PCs).

Für Regel 7 und 8 werden alle Adressen ("Any address") für jeglichen Datenverkehr gesperrt. Unter diese Regel fallen dann alle Verbindungsversuche, die nicht bereits von Regel 5 und 6 für JuNet-internen Datenverkehr erfaßt wurden.

Nach Definition der Regeln müssen diese in der Liste mit Hilfe der Pfeiltasten rechts unten in die richtigen Positionen 1 bis 8 gebracht werden.



Alle weiteren Regeln sind für dieses Beispiel dann nicht mehr relevant und können auch durch Anklicken der Auswahlbox deaktiviert werden.

28 April 2000

J.Meißburger, Forschungszentrum Jülich, FZJ-ZAM, dokumentation.zam@fz-juelich.de