



*@Guard*



*Personal Firewall*

*j.meissburger@fz-juelich.de*

Für Windows-Systeme  
**außer Windows -ME und XP** geeignet



*ein Webfilter und  
persönliches Firewall für Internet-PCs*

ZAM technische Kurzinformation

ZAM-TKI-0349 (AtGuard)

und interner Bericht

ZAM-IB-9916



<http://www.fz-juelich.de/zam/net/security>

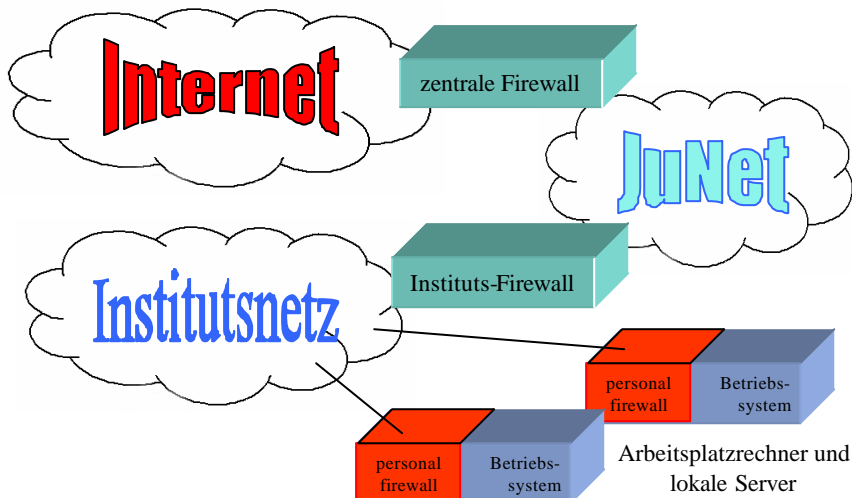


## Funktionen eines IP-Firewalls

- Filtern und Steuern des IP- und ICMP-Verkehrs nach Adressen und Domänen
- Filtern und Steuern der Anwendungen nach IP-Ports (Dienste) und Anwendungen
- Unterscheidung von einlaufendem („inbound“) und auslaufendem („outbound“) Datenverkehr
- Erkennen besonderer, potentiell gefährlicher Dateninhalte
- Verbergen oder Umschreiben von Netzadressen (address translation)
- Logische Verknüpfung von durch Filterregeln definierten Ereignissen
- Logging von Ereignissen und Statistik



## Die Anordnung von Firewalls im Firmennetz





## Firewalls

- Ein Schutzwall für IP-Kommunikation zwischen
  - Firmen-Firewall: Zwischen dem weltweiten Internet und dem lokalen Firmennetz am zentralen Zugangspunkt zum Internet (Internet ↔ JuNet)
  - Abteilungs-Firewall: Zwischen dem firmenweiten Netz und dem lokalen Netz, in dem sich der eigene Rechner befindet (JuNet ↔ zamnet)
  - Persönliche Firewall: Zwischen dem lokalen Hausnetz und dem eigenen Rechner (zamnet ↔ ZAM-Rechner)
- Eine persönliche Firewall schützt auch
  - gegen ungewollte Kommunikation im eigenen Hausnetz, beispielsweise durch falsch konfigurierte Rechner oder durch Neugier von Kollegen
  - vor allem gegen Angriffe, die von Rechnern im eigenen Netz ausgehen, die bereits von Hackern „übernommen“ worden sind
  - häufig auch gegen Gefährdung durch unvorsichtige Navigation im Web (Skripting, aktive Inhalte)



## persönliche (Desktop) Firewalls

- Tiny Personal Firewall
  - <http://www.tinysoftware.com>
- ConSeal PC-Firewall
  - <http://www.candel.com/conseal>
- ZoneAlarm
  - <http://www.zonealarm.com>
- Norton Personal Firewall 2002
  - [http://www.fz-juelich.de/zam/docs/tki/tki\\_html/t0376/t0376.html](http://www.fz-juelich.de/zam/docs/tki/tki_html/t0376/t0376.html)
- **AtGuard (lizenziert für FZJ, verfügbar auf \\zelcds\atguard )**
  - [http://www.fz-juelich.de/zam/docs/tki/tki\\_html/t0349/t0349.html](http://www.fz-juelich.de/zam/docs/tki/tki_html/t0349/t0349.html)
  - <http://www.fz-juelich.de/zam/docs/printable/ib/ib-99/ib-9916.pdf>

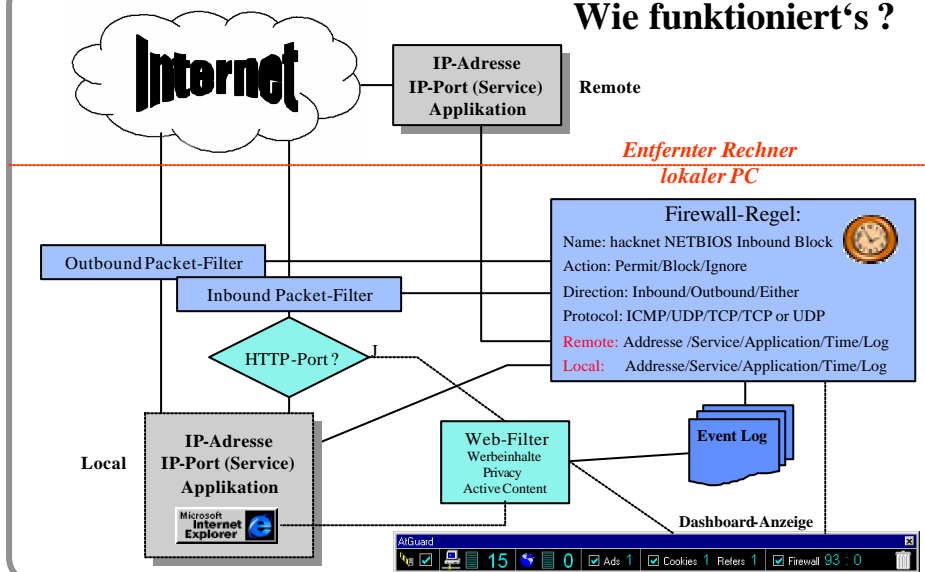


## Was ist AtGuard?

- Ein Monitor- und Statistikwerkzeug für ein- und ausgehende IP-Verbindungen (Dashboard, Regel- und Filter-Assistent, Eventlog).
- Ein regelbasiertes Firewall für ICMP- und IP-Pakete. Berücksichtigt werden:
  - Quell- und Zieladresse
  - Art des Dienstes (Quell- und Ziel-IP-Port)
  - Die dienstvermittelnde Applikation
  - Wochentag und Uhrzeit
- Ein Webfilter für:
  - Werbeinhalte (Inbound)
  - Persönliche Benutzerinformationen (Outbound)
  - Aktive, potentiell gefährliche Web-Inhalte (Inbound Scripting, ActiveX, Java)
- Ein Alarmierungswerkzeug für unerwünschte Verbindungsversuche



## Wie funktioniert's ?



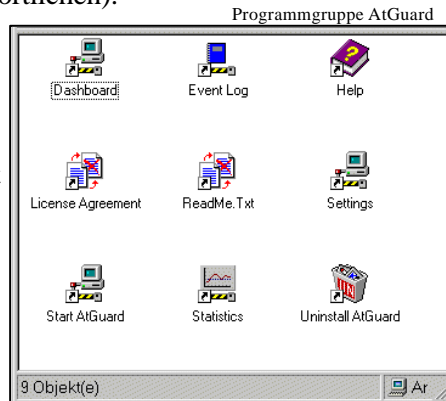


## Die Installation der Software





- Den Softwarekit \\zslcds\atguard\ATGD322.EXE und **Readme.txt** auf ein temporäres Verzeichnis C:\TEMP herunterladen (Anmelden mit UserID/Passwort des PC-Verantwortlichen).

- **Readme.txt** lesen und C:\TEMP\ATGD322.EXE ausführen:  
Next - Yes - Next - Next - Next  
Reboot

- Installationskit C:\TEMP\ATGD322.EXE löschen oder für eine eventuelle Nachinstallation aufbewahren



## Die Bedeutung der Programmelemente

- **Help, ReadMe.txt und License Agreement:** Hinweise zur Benutzung
- **Settings:** Konfiguration von Programmstart, Firewall und Webfiltern  
 *Dieses Programm muß als erstes aufgerufen werden !*
- **Start AtGuard:** Start des Programms und der Filterfunktionen
- **Dashboard:**

 zentrales Steuer- und Anzeigeelement für IP-Verbindungen und Statistik
- **Event Log:** Protokoll aller IP-Verbindungen und der durch Ansprechen der Filter und Firewall-Regeln ausgelösten Aktionen
- **Statistics:** Verkehrsstatistik zu IP- und Webverbindungen (Summary)
- **Uninstall AtGuard:** Vollständige Deinstallation des Programms
- **Taskbar-Icon:** @Guard aktiviert  oder deaktiviert 



## Starteinstellungen in „Settings“

- Optionen für den Programmstart und den Routinebetrieb

Einstellungen für den Routinebetrieb mit stabiler Konfiguration

Dashboard kann auch jederzeit im laufenden Betrieb ein- und ausgeschaltet werden

Paßwortschutz erst nach endgültiger Konfiguration einschalten !

Erst nach durchgeführter Konfiguration einschalten !

AtGuard beim Booten automatisch starten !



## Das „Dashboard“



- Zentrales Anzeige- und Steuerelement für Webfilter und Firewall und Alarmanzeige für die Firewall:

- Wie die Windows -Taskleiste am oberen Bildrand „gedocked“, verschwindet auf Wunsch automatisch im Hintergrund
- Zeigt Zähler für Webseiten, geblockte Ad's, Cookies, Referrers und ausgewertete Firewall-Regeln (permitted/blocked)

- Zeigt die zur Zeit aktiven Ports und Verbindungen
- und für jede Verbindung die Zahl übertragener Bytes

Proto	Executable	State	Remote	Local	Sent	Received	Time
TCP	inetinfo.exe	Listening		zem125: http	0	0	1:39:49
TCP	inetinfo.exe	Listening		localhost: 1027	0	0	1:39:53
TCP	inetinfo.exe	Listening		zem125: 1028	0	0	1:39:52
TCP	RPCSS.EXE	Listening		zem125: 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		zem125: nbssession	0	0	1:40:01
TCP	war-ftp.exe	Listening		zem125: ftp	0	0	1:39:44
UDP	explorer.exe	Listening		localhost: 1047	67	67	1:28:44
UDP	RPCSS.EXE	Listening		zem125: dcom	0	4080	1:39:54
UDP	System	Listening		zem125: nbname	476	67370	1:40:01
UDP	System	Listening		zem125: nbdatagram	2427	152688	1:40:01
UDP	war-ftp.exe	Listening		zem125: 1033	0	0	1:39:44
UDP	war-ftp.exe	Listening		zem125: portmap	0	88	1:39:44



## Ein besonders interessantes Beispiel ....

- Anzeige der Verbindungen mit „netstat -an“ unter Win95a
- und Anzeige im Dashboard von AtGuard:

```
Microsoft(R) Windows 95
(C) Copyright Microsoft Corp 1981-1995.

Win95_C:\>netstat -an

Active Connections

Proto Local Address           Foreign Address
UDP   134.94.169.167:137    *:*UDP   134.94.169.167:138    *:*Win95_C:\>
```

Proto	Executable	State	Remote	Local	Sent	Received	Time
TCP	MPREXE.EXE	Listening		zam015.zam.kfa-juelich.de: nbssession	0	0	2:18
TCP	MTMTASK.DL	Listening		zam015.zam.kfa-juelich.de: Backdoor-g-3	0	0	51
TCP	MTMTASK.DL	Listening		zam015.zam.kfa-juelich.de: Backdoor-g-1	0	0	51
TCP	MTMTASK.DL	Listening		zam015.zam.kfa-juelich.de: Backdoor-g-2	0	0	51
TCP	NBSVR.EXE	Listening		zam015.zam.kfa-juelich.de: NetBus-Pro	0	0	1:55
UDP	MPREXE.EXE	Listening		zam015.zam.kfa-juelich.de: nbdatagram	0	0	2:18
UDP	MPREXE.EXE	Listening		zam015.zam.kfa-juelich.de: nbname	816	816	2:18

Trojaner Sub Seven

Trojaner NetBus-Pro



## Das Event-Log

- Loggen aller durch @Guard erfaßten Netzwerk-Ereignisse, insbesondere die Auswertung von Alarm-Regeln des Firewalls

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

- Log der Verbindungen mit Datum, Uhrzeit, Adressen und Byte-Statistik

- Details einer über den Regelassistenten des Firewalls explizit zugelassenen Verbindung

20.10.99 10:14:44.789 Rule "JuNet HTTP permit / log" permitted (zam125:http). Details:

19.10.99 15:27:54.423 Interactive learning mode is enabled

19.10.99 15:27:54.423 Firewall is enabled. It has successfully processed a total of 21 rules

19.10.99 14:28:39.331 This one time, the user has chosen to "permit" communications. Details:

19.10.99 14:28:15.297 Interactive learning mode is enabled

This one time, the user has chosen to "permit" communications. Details:

Inbound TCP connection  
Local address,service is (zam125:ftp)  
Remote address,service is (zam329.zam.kfa-juelich.de,33033)  
Process name is "war/tpd.exe"



# Die Verkehrsstatistik

**Netzwerk-Gesamtraten**

**Webfilter**

**Effizienzgewinn durch Webfilter: nicht sinnvoll für LAN!**

**Firewall TCP-Statistik**

**Firewall UDP-Statistik**

**Regelstatistik**

**Verbindungsstatistik**

**Echtzeitanzeige**

Proto	Executable	Remote	Local	Sent	Recv	Time
IEXPLORE	E...	ftp.klo.waelch...	zsm125.2828	45	183	24
IEXPLORE	E...	ftp.klo.waelch...	zsm125.2831	45	183	19
IEXPLORE	E...	ftp.klo.waelch...	zsm125.2832	100	324	15
TCP	IEXPLORE E...	zsm125.ftp	zsm125.2815	1728	432	1.01
TCP	IEXPLORE E...	zsm125.ftp	zsm125.2816	593	144	1.01
TCP	IEXPLORE E...	zsm125.ftp	zsm125.2817	295	72	1.01
TCP	IEXPLORE E...	zsm125.ftp	zsm125.2818	295	72	1.01



# @Guard als Webfilter

Ad-Blocking

Privacy

Active Content



## Die Funktion als Webfilter

- **Ad-Blocking:** Aussieben bestimmter HTML-Inhalte durch Zeichenketten-basierten Vergleich mit einer Filterliste
- **Privacy:** Verhindern der Weitergabe von Benutzer-bezogenen Browserinformationen an den Webserver
- **Active Content:** Verhindern der Ausführung potentiell gefährlicher Webinhalte wie Scripting, ActiveX und Java.  
Abbrechen von Grafikanimationen nach einem Durchlauf
- Verwalten individueller Einstellungen für Ad-Blocking, Privacy und Active Content für unterschiedliche IP-Domänen und Rechner
- Konfiguration zusätzlicher Webserver-Ports außer dem Standardport 80



## Domänenkonzept für Webfilter

**Ein/Ausschalten *aller* Webfilter**

**Spezielle Konfiguration für einzelne Rechner oder IP-Domänen**

**Definition der zu blockierenden oder für Unterdomänen zu erlaubenden HTML-Masken**

**Achtung: Defaults gelten immer!**

**Domäne oder Rechner hinzufügen**

**HTML-Maske hinzufügen**

**Webfilter-Options**

Action	HTML string
Block	#CLink
Block	%23CLink
Block	%2Fads%2E
Block	%3Fad%2E
Block	&ad_
Block	&banner=
Block	-ad.cgi
Block	-ads/
Block	ad.
Block	ads.
Block	ads/
Block	.anm
Block	.net-on.com
Block	.net-on.com



## Webfilter-Optionen

Filters...

Hier können die Filter für  
Ad blocking  
Privacy  
Active Content  
einzeln aktiviert/deaktiviert werden


Diese IP-Ports werden als  
HTTP-Dienste betrachtet und  
durch die Webfilter gefiltert

**Assistent für Cookies:**  
Besser abschalten, Cookies sind  
häufig und harmlos!

**Assistent für aktive Inhalte:**  
Damit können **interaktiv** Domänen- oder Host-  
spezifisch aktive Inhalte (Scripting, Java,  
ActiveX) zugelassen oder blockiert werden



## Ad-Blocking (HTML-Filter)

- Ausfiltern bestimmter HTML-Inhalte durch Zeichenketten-Filter, z.B.
  - **Dateien und Dateipfade:** `ad, -ads, /adimages/, /sponsors/, &banner=`
  - **Numerische IP-Adressen:** `/199.78.52`
  - **Unicode-Textstrings:** `%3FAd%2E,`
  - **DNS-Namen und Domänen:** `www.marketspace, yahoo.com/adv, bannerpower.com`
- Die Liste vordefinierter Filter entspringt dem englischsprachigen Raum und muß ggf. durch deutschsprachige Zeichenketten erweitert werden
- Die Defaults-Liste gilt für alle Domänen, kann aber mit „Add“ durch „Permit“-Einträge in einer Unterdomäne überschrieben werden
- Neue Filtereinträge können halbautomatisch und interaktiv durch Kopieren eines Links aus einer angezeigten HTML-Seite in den Mülleimer (Trashcan) des Dashboards  erstellt werden



## Ein Web-Filter mit dem Dashboard erstellen im Forschungszentrum Jülich

- Beispiel: Ein Element auf der Homepage von [www.fz-juelich.de](http://www.fz-juelich.de)

1 Rechte Maustaste auf Bild klicken  
„Kopieren“

2 Rechte Maustaste auf Müllimer  
„Paste into Trashcan“

3 Filter bestätigen oder modifizieren



## Privacy-Filter

- Die Privacy-Filter verhindern die Weitergabe von lokal konfigurierten Benutzerdaten („Extras - Internetoptionen - Inhalt - Profil“ im IE):
- Drei Einstellmöglichkeiten: „Block, Permit und Reply“

Die Einstellung „Cookies“ legt fest, ob Cookies lokal abgelegt werden dürfen bzw. welchen Text der Browser bei Anforderung eines Cookies statt dessen zurücksendet

Referer-Feld: Adresse der zuletzt besuchten HTML-Seite

Browser-Feld: Bekanntgabe des benutzten Browsertyps

Email-Feld: Bekanntgabe der eigenen Email-Adresse



## Active Content

- Domänen-spezifische Filterung potentiell gefährlicher Webinhalte wie Active Scripting, PopUp-Windows, Java und ActiveX

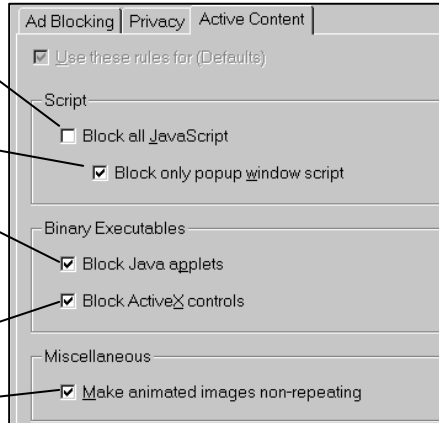
**Blockieren aller**  
`<script language=.....></script>` Inhalte,  
 vor allem für JavaScript und VBScript

**Verhindern von PopUp-Fenstern mit**  
`var newwin = window.open(...)`

**Unterbinden des Ladens und der**  
**Ausführung von Java -Applets**  
`<applet code="javaclass.class">... </applet>`

**Blockieren des Ladens und der**  
**Ausführung von ActiveX-Steuer-elementen**  
`<object classid="clsid:.....">.....</object>`

**Animierte Grafiken nach einem**  
**Durchlauf „einfrieren“ (animated GIFs)**



## Der Java/ActiveX-Assistent

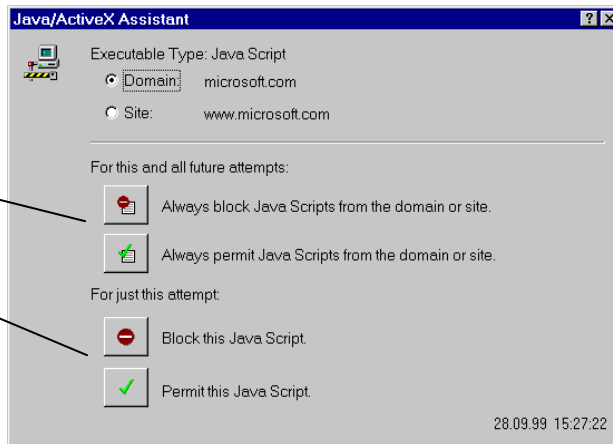
- Durch einfachen Mausklick kann die Ausführung aktiver Inhalte für eine IP-Domäne oder einen einzelnen Webserver (Site) verhindert oder zugelassen werden

- Die Entscheidung kann

- permanent
- oder

- nur für diese Browsersitzung

gefällt und gespeichert werden



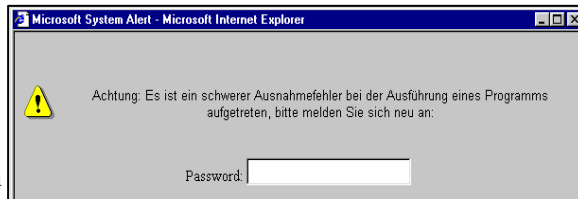


## Warum zusätzliche Filter ?

- Scripting, ActiveX und Java können durch die Sicherheitseinstellungen im Internet-Explorer detaillierter gesteuert werden als mit @Guard.
- Deshalb die @Guard-Filter **ergänzend für andere Anwendungen als den IE**, wegen der zusätzlichen Filter (PopUp, animated GIF) oder dann benutzen, wenn die IE-Filter nicht zur Verfügung stehen
- Animierte Grafiken können, wenn der Browser auf einem Server läuft (NT-Terminalserver oder WinCenter von NCD) unnötige und recht hohe Netzlast verursachen
- PopUp-Fenster enthalten oft nur störende Reklameinformation, sie können aber auch für

„**human engineering**“-  
**Attacken**

wie etwa zum Ausspähen  
von Paßwörtern  
mißbraucht werden



## *@Guard als Firewall*

**Applikationsfilter**

**Portfilter**

**Adreßfilter**

**Zeitplanung**

**Logging**



## Die Funktionsweise des Firewalls

- Für jede einlaufende („Inbound“) oder auslaufende („Outbound“) IP-Verbindungsanforderung oder ICMP-Meldung wird die Liste der als aktiv markierten Regeln **sequentiell von oben nach unten** durchlaufen
- Sobald eine Regel zutrifft („match“), wird ein der Aktionen
  - **Permit:** Verbindung zulassen
  - **Block:** Verbindung nicht zulassen
  - **Ignore:** Verbindung ignorieren, ggf. loggen und Regelliste weiter durchsuchen ausgeführt und das Durchsuchen der Regelliste - außer bei „Ignore“ - abgebrochen
- Wird keine passende Regel gefunden, so wird (falls aktiviert) der **Regelassistent** gestartet
- Eine Verbindung, für die keine gültige Regel gefunden wurde, wird bei nicht aktiviertem Regelassistenten **per Default abgelehnt!**



## Das „Regelwerk“: Die Regelliste

The screenshot shows the 'AtGuard Settings' window with the 'Firewall' tab selected. The 'Enable firewall' checkbox is checked. Below it, a list of 'Firewall Rule' entries is shown, each with a checkbox and a 'Rule Action Summary' column. The rules include 'NTP Time Sync', 'Localhost Default permit', 'zam125 Default permit', 'zam125 Default ICMP permit', 'JuNet ICMP Default Outbound permit', 'JuNet Outbound permit', 'Default DNS Permit', 'jnpc01 (RAS) ICMP Default Permit', 'jnpc01 (RAS) Default permit', 'zam406 ICMP Default permit', 'zam406 Default permit', 'JuNet ICMP Echo permit', 'zammon WebTermX (wbx2.exe) X11 Permit', 'WINS nbdatagram/nbname permit', 'PCSRV nb\_all permit', 'ADSMPCSRV Permit', and 'zsmnet nbdatagram/nbname permit'. The 'Rule Action Summary' column shows various actions like 'ntp zam.kfa-juelich.de: ntp.time', 'localhost', 'zam125 zam.kfa-juelich.de', etc. At the bottom, there are buttons for 'Add...', 'Modify...', 'Remove', 'Test...', and arrows for reordering. The 'Test...' button is highlighted with a callout.

**Firewall komplett ein- oder ausschalten**

**Interaktiven Regelassistenten ein- oder ausschalten**

**Liste der sequentiell durchlaufenen Regeln**

**temporär deaktivierte Regeln**

**Hinzufügen, Löschen und Modifizieren von Regeln**

**Regeltest**

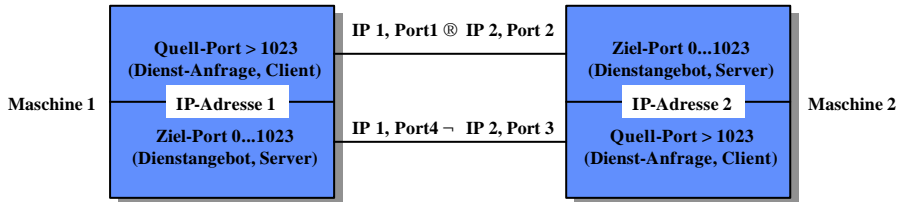
**Richtung und Art des gefilterten Verkehrs**

**Reihenfolge einer Regel in der Liste verändern**



## Zur Erinnerung: IP-Kommunikation

- Ein IP-Verbindung zwischen zwei Maschinen wird über "IP-Sockets" mit Hilfe der WinSock-Schnittstelle (WSOCK32(N).DLL) hergestellt:



- Ein Server bietet Dienste im Netz an, indem ein Programm (ein "Dienst") auf einem ganz bestimmten IP-Port (TCP oder UDP) "lauscht"
- Ein Client versucht
  - sich mit diesem Port zu verbinden ("SYNC") und dann über die stehende Verbindung Daten auszutauschen (verbindungsorientiert, TCP)
  - oder einfach Pakete an den Port zu senden und zu hoffen, daß diese ankommen (verbindungslos, UDP)



## Erstellen einer neuen Regel

### Name der neuen Regel

(Namensgebung möglichst standardisieren)

### Auszuführende Aktion:

- Permit
- Block
- Ignore

### Kommunikationsrichtung:

- Inbound
- Outbound
- Either

### Protokoll:

- TCP
- UDP
- TCP or UDP
- ICMP

Verbindungsdetails: Anwendung Dienst (IP-Port) IP-Adressen Zeitplanung Logging



## Anwendung und IP-Dienst (Port)

- **Application**
  - Spezifiziert eine spezielle Applikation, auf die sich der Verbindungswunsch bezieht. Angabe im allgemeinen nicht erforderlich („Any Application“), da ein Dienst meist eindeutig durch seinen IP-Port gekennzeichnet ist.
- **Service (Dienst, IP-Port)**
  - Lokaler und entfernter Service-Port
  - Beispiel: HTTP-Dienst (Webserver) auf dem lokalen PC (http = Port 80)
- **Port/Namenszuordnung:**
  - Interne Liste von AtGuard, siehe HELP „AtGuard Port and Service Assignments“
  - Windows NT:  
C:\%SystemRoot%\system32\drivers\etc\Services
  - Windows 95/98:  
C:\%SystemRoot%
- Auch „non-listening ports“ werden erfaßt und gefiltert!

Application	Service	Address	Time Active	Logging
Remote Service		Local Service		
<input type="radio"/> Single service <input type="radio"/> Service range <input type="radio"/> List of services <input checked="" type="radio"/> Any service		<input checked="" type="radio"/> Single service <input type="radio"/> Service range <input type="radio"/> List of services <input type="radio"/> Any service		
		Service name or port:		
		http		

Dienst (Port) auf dem entfernten Server

Dienst (Port) auf dem lokalen PC



## IP-Adressen der Kommunikationspartner

- **Host-Adresse eines einzelnen Rechners:**
  - **IP-Adresse numerisch:** 134.94.100.72
  - **IP-Hostname:** www.fz-juelich.de
- **Netzwerk-Adresse eines Subnetzes (Subnetzmaske) oder Teilnetzes:**
  - **Network address** (Netz/Subnetzmaske):
    - **JuNet:** 134.94.0.0 / 255.255.0.0
    - **zamnet2:** 134.94.168.0 / 255.255.248.0
  - **Address range** (Teilnetz):
    - **Teilbereich aus JuNet-RAS:** 134.94.114.2 - 134.94.114.254
- **Jede Adresse:**
  - alle IP-Adressen werden berücksichtigt
- Für den lokalen PC mit einem Interface und ohne virtuelle Server kann im allgemeinen „Any address“ (= IP-Adresse des PCs) eingetragen werden

Application	Service	Address	Time Active	Logging
Remote Address		Local Address		
<input type="radio"/> Host address <input checked="" type="radio"/> Network address <input type="radio"/> Address range <input type="radio"/> Any address		<input type="radio"/> Host address <input checked="" type="radio"/> Any address		
Address:		134.94.0.0		
Subnet mask:		255.255.0.0		



## Zeitabhängige Regeln

- Regeln können zeitabhängig aktiviert/deaktiviert werden
- Beispiel: Zugang nur während der Dienstzeit, nicht an Wochenenden, Freitag bis Mitternacht für Backup

Application	Service	Address	Time Active	Logging
This rule will be active for the time intervals shown:				
Sunday:			Never	⬇
Monday:			08:00 -> 17:00	⬇
Tuesday:			08:00 -> 17:00	⬇
Wednesday:			08:00 -> 17:00	⬇
Thursday:			08:00 -> 17:00	⬇
Friday:			08:00 -> 23:59	⬇
Saturday:			Never	⬇

Montag - JuNet HTTP permit / log

Start time: 08:00

End time: 17:00

00:00	:00
01:00	:05
02:00	:10
03:00	:15
04:00	:20
05:00	:25
06:00	:30
07:00	:35
08:00	:40
09:00	:45
10:00	:50
11:00	:55
12:00	
13:00	
14:00	
15:00	
16:00	
17:00	
18:00	
19:00	
20:00	
21:00	
22:00	
23:00	
23:59	

Apply this time interval to every day of the week.



## Logging

- Die Verbindungsdetails beim Ansprechen einer Regel können im Eventlog gespeichert oder es kann ein Alarm ausgelöst werden
- Dies empfiehlt sich vor allem für Ressourcensensitive Ports wie
  - NBSESSION (Port 139)
  - FTP control (Eigener FTP-Server, Port 21)
  - DCOM (Port 135)
  - Portmapper (Port 111)
  - HTTP (Eigener Webserver, meist Port 80)
- Die Einträge werden im Eventlog unter „Firewall“ abgespeichert:

Application	Service	Address	Time Active	Logging
<input checked="" type="checkbox"/> Write an event log entry when this rule is matched. Log event after: 1 matches. <input type="checkbox"/> Show notification in the dashboard when this rule is logged.				

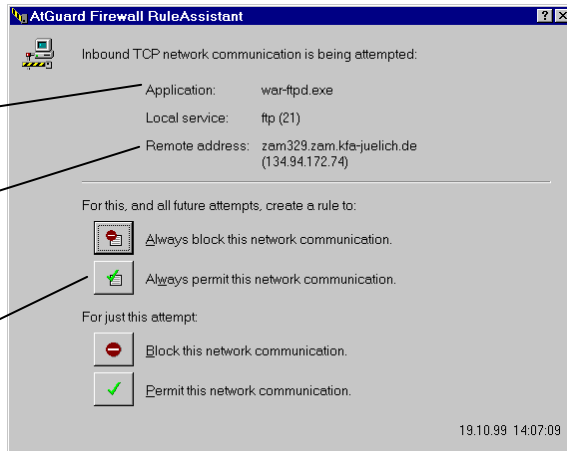
Hier werden auch Start und Stop des Firewalls protokolliert!

20.10.99	10:14:44.789	Rule "JuNet HTTP permit / log" permitted (zam125.http). Details:		
19.10.99	15:27:54.423	Interactive learning mode is enabled		
19.10.99	15:27:54.423	Firewall is enabled. It has successfully processed a total of 21 rules		
19.10.99	14:28:39.331	This one time, the user has chosen to "permit" communications. Details:		
19.10.99	14:28:15.297	Interactive learning mode is enabled		
This one time, the user has chosen to "permit" communications. Details:				
Inbound TCP connection				
Local address.service is (zam125.tp)				
Remote address.service is (zam323.zam.kfa-juelich.de.33033)				
Process name is "war-ftp.exe"				



## Erstellen einer Regel mit dem Regelassistenten

- Beispiel: Verbindungsversuch vom eigenen Unix-Rechner zu einem lokal auf dem PC laufenden FTP-Server (war-ftpd) auf Port 21 (FTP Control Port)
- Verbindung nur zu diesem (sicheren) FTP-Server zulassen
- Autorisierter Rechner
- Diese Verbindung soll auch in Zukunft immer zugelassen werden



## Schritt für Schritt ....

This wizard will help you create a firewall rule that permits inbound TCP network communication. You will be asked to make choices about the following rule properties:

Application: war-ftpd.exe (1)  
 Local service: ftp, port 21 (2)  
 Remote address: zam329.zam.kfa-juelich.de (3)

To begin, select the communication you wish to permit:

While an event occurs when communication matches the rule

Rule summary: Inbound TCP communication from zam329.zam.kfa-juelich.de to local service ftp (4)

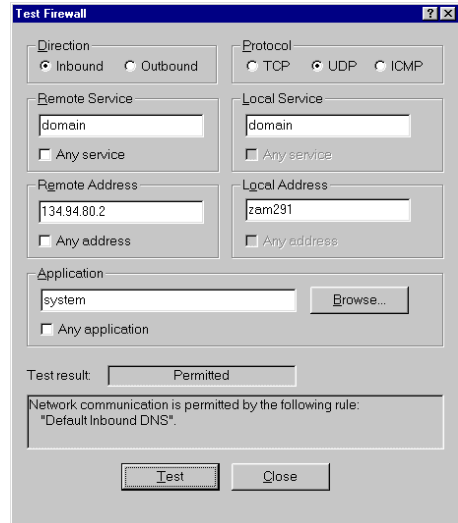
Next (6)

- Die fertige Regel wird in die Regelliste eingetragen (6)

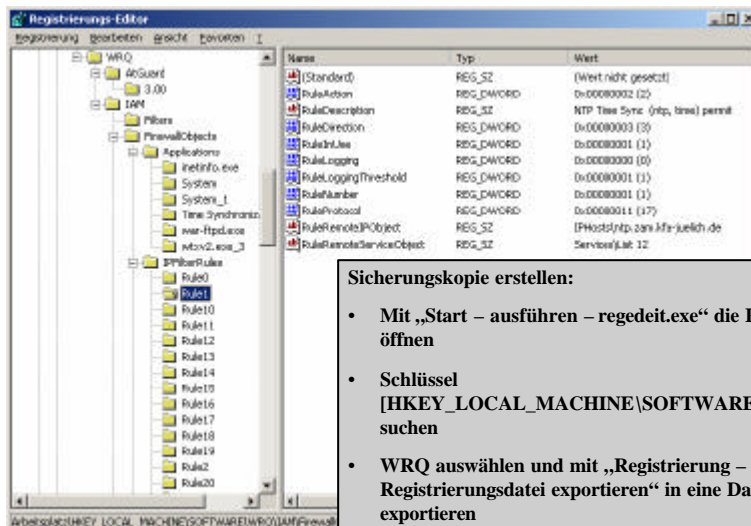


## Testen einer Regel

- Test einer Regel durch Simulation eines Verbindungsversuchs
- Beispiel: Testen einer JuNet-Nameserver-Rückfrage beim eigenen PC:
  - Nameserver-Adresse: 134.94.80.2
  - Dienst: domain, Port 53 / UDP
  - lokale Adresse: zam291
  - Dienst: domain, Port 53 / UDP
  - Applikation: System
- Die Kommunikation wird durch die Regel „Default Inbound DNS“ (also eine allgemeinere, aber „richtige“ Regel) zugelassen



## AtGuard-Einstellungen in der Registry





## *Regeln für JuNet*

**Kommunikation nur lokal**  
**Kommunikation mit einem Server**  
**Offene Intranet-Kommunikation**  
**Kommunikation im Hausnetz**



## **Grundsätzliche Vorgehensweise**

- Startkonfiguration je nach Kommunikationsbedarf auswählen
- Spezielle, immer benötigte Dienste mit „Permit“ zuerst eintragen
- Zeitkritische und häufig benötigte Dienste (Zeitsynchronisation, lokale Kommunikation, DNS-Dienste) an den Listenanfang stellen
- Unerwünschte, spezielle Kommunikationstypen (bestimmte Hosts, bestimmte Dienste) anschließend eintragen
- Allgemeinere, z.B. Netzwerk-weit gültige Regeln zum Schluß eintragen, damit spezifischere Regeln nicht logisch überschrieben werden
- Regelasistenten aktivieren und beobachten, weitere Permits einrichten und in der Regelliste oberhalb der „Block“-Regeln anordnen
- Häufige, unerwünschte Dienstanforderungen (meist aus dem Intranet) explizit als spezielle Regel mit Hilfe des Assistenten nachtragen



## Der „geschlossene“ PC

- Netzwerk eingerichtet, aber keinerlei Kommunikation im Netz
- Regelasistent abgeschaltet!
- Volle lokale IP-Kommunikation z.B. für die Entwicklung und den Test von Websites (CGI'S, ASP's) oder anderer Client/Server-Anwendungen
- Default-Kommunikation mit **localhost = 127.0.0.1**
- Default-Kommunikation mit eigener IP-Adresse „myclient“
- Namensauflösung für eigenen Rechner nicht durch Nameserver (BIND), sondern durch lokale Hosts-Datei (oder mit numerischer IP-Adresse):
  - Windows NT: C:\%SystemRoot%\system32\drivers\etc\Hosts
  - Windows 95/98: C:\%SystemRoot%\Hosts
  - mit den Einträgen: 127.0.0.1 localhost  
134.94.xxx.xxx myclient

Pos	Name	Action	Dir.	Protocol	Appl.	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



## Kommunikation mit einem Server

- Kommunikation nur mit einer bestimmten, als vertrauenswürdig eingestuften („Hacker“-freien) Maschine „myserver“
- Regelasistent abgeschaltet!
- Verwendung numerischer IP-Adressen oder Namensauflösung durch lokale Hosts-Datei (localhost, myclient, mysverver...)
- Statt „Myserver Default Permit“ können zur Erhöhung der Sicherheit auch nur einzelne, auf dem Server benutzte Dienste eingetragen werden

Pos	Name	Action	Dir.	Protocol	Appl.	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 Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	myserver / Any
4	MYSERVER ICMP Default Permit	Permit	Either	ICMP	-	Any Type	myserver / Any



## Der „JuNet-PC“ für das Intranet

- Lokale (systeminterne) Default-Kommunikation zulassen
- Abblocken besonders gefährlicher „Backdoors“ wie Back Orifice, NetBus und PC-Anywhere mit Logging und Alarm
- ICMP-Meldungen aller Typen (Ping, Router-Meldungen etc.) innerhalb JuNet [134.94.0.0, Netzmaske 255.255.0.0] zulassen
- Default (alle) TCP- und UDP-Kommunikation innerhalb JuNet zulassen

Pos	Name	Action	Dir.	Protocol	Appl.	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	Back Orifice Block / log / alarm	Block	Either	TCP or UDP	Any	Any / Back Orifice, Back Orifice 2000	Any / Any
4	NetBus Block / log / alarm	Block	Either	TCP or UDP	Any	Any / NetBus, NetBus Pro	Any / Any
5	PC-Anywhere Block / log / alarm	Block	Either	TCP or UDP	Any	Any / PC-Anywhere-Data, PC-Anywhere-Status	Any / Any
6	JUNET ICMP Default Permit	Permit	Either	ICMP	-	Any Type	JuNet / Any
7	JUNET Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	JuNet / Any



## Individuelle Konfiguration in JuNet, Teil 1 (Permit)

- Kommunikation mit
  - Sich selbst (LOCALHOST, MYCLIENT) und dem eigenen Home-PC mit Rechnern im hausinternen Subnetz (MYNET)
  - mit einem Server (MYSERVER) außerhalb des eigenen Netzes
  - und mit wichtigen Servern im JuNet wie:

NTP	Time Server (ntp, time)
DHCP	Dynamic Host Configuration Server
DNS	Distributed Name Service (domain)
WINS	Windows Internet Names Service (nb)
PCSRV	PC-Server des ZAM (nb)
ZELCDS	PC-Server des ZEL (nb)
IMAPSRV, POPSRV	Mailserver (imap, imap-ssl, pop3)
MAILRELAY	Mailgateway (smtp)
HTTP, HTTPS	WWW-Server des FZJ
ADSMPCSRV, BACKUPSRV	Tivoli-Backupserver



## Detailkonfiguration „Permit“

1	NTP Time Sync (ntp, time) Permit	Permit	Either	UDP	Any	ntp, time / Any	ntp.zam / Any
2	LOCALHOST Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	localhost / Any
3	MYCLIENT Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	myclient / Any
4	Domain Default Permit	Permit	Either	UDP	Any	domain / Any	Any / Any
5	MYCLIENT ICMP Default Permit	Permit	Either	ICMP	-	Any Type	myclient / Any
6	MYNET ICMP Default Permit	Permit	Either	ICMP	-	Any Type	mynet / Any
7	MYNET Default Outbound Permit	Permit	Out	TCP or UDP	Any	Any / Any	mynet / Any
8	HOMEPC Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	myhomepc / Any
9	HOMEPC ICMP Default Permit	Permit	Either	ICMP	-	Any Type	myhomepc / Any
10	IMAP mailserver	Permit	Out	TCP or UDP	Any	imap-ssl, imap, 8000, pop3 / Any	imapsrv.fz-juelich.de / Any
11	MAILRELY Default Permit	Permit	Either	TCP or UDP	Any	smtp / Any	mailrelay.fz-juelich.de / Any
12	WINS nbdata/nbname Permit	Permit	In	TCP or UDP	Any	Any / nbname, nbdatagram	wins.zam / Any
13	PCSRV nb_all Permit	Permit	In	TCP or UDP	Any	nbdatagram, nbname, nbession / Any	pcsrv.zam / Any
14	DHCP/BOOTP	Permit	Either	UDP	Any	bootpc,bootps/bootps,bootpc	zam467, zam468
15	BACKUPSRV Default Permit	Permit	Either	TCP or UDP	Any	Any / Any	adsmcpsrv.zam / Any



## Detailkonfiguration „Block“

- Verhindern der Kommunikation mit
  - den Remote-Access-Servern für JuNet (Modem- und ISDN-Server)
  - den bekannten Backdoors Back Orifice, NetBus und PC-Anywhere mit Alarmauslösung
  - häufigen, aber im allgemeinen unerwünschten Service-Anfragen wie SNMP, ICMP, PORTMAP oder DCOM (nur bei aktivem Regelassistenten erforderlich)
- Logging für 21-24 kann je nach Umfeld zu vielen Eventlog-Einträgen führen, deshalb ggf. nach Identifikation der Verursacher abschalten

16	JUNET RAS1 Default Block	Block	In	TCP or UDP	Any	Any / Any	134.94.114.0 255.255.254.0 / Any
17	JUNET RAS2 Default Block	Block	In	TCP or UDP	Any	Any / Any	134.94.112.0 255.255.255 / Any
18	Back Orifice Block / log / alarm	Block	Either	TCP or UDP	Any	Any / Back Orifice, Back Orifice 2000	Any / Any
19	NetBus Block / log / alarm	Block	Either	TCP or UDP	Any	Any / NetBus, NetBus Pro	Any / Any
20	PC-Anywhere Block / log / alarm	Block	Either	TCP or UDP	Any	Any / PC-Anywhere-Data, PC-Anywhere-Status	Any / Any
21	ICMP Router Advertisement Block	Block	In	ICMP	Any	router advertisement	Any / Any
22	Default SNMP Block	Block	In	TCP or UDP	Any	Any / snmp	Any / Any
23	Default PORTMAP (111) Block	Block	In	TCP or UDP	Any	Any / portmap	Any / Any
24	Default DCOM (135) Block	Block	In	TCP or UDP	Any	Any / dcom	Any / Any



## Noch einige Tipps...

- Am besten ist eine detaillierte, mit Hilfe expliziter Regeln individuell angepaßte Konfiguration mit aktiviertem Regelassistenten. Nur so bekommt man wirklich mit, was läuft .....
- Von Zeit zu Zeit und nach Einfügen einer neuen Regel sollte man die Reihenfolge überprüfen und/oder die Regel explizit testen!
- Das Eventlog sollte regelmäßig nach auffälligen Einträgen überprüft werden, vor allem bei deaktiviertem Regelassistenten.
- Nach Regelkonsolidierung Paßwortschutz aktivieren!

