



**Symantec**



**Norton Personal  
Firewall 2002**

*auch enthalten in  
Symantec Internet Security*

*j.meissburger@fz-juelich.de*



**ein Webfilter und  
persönliches Firewall für Internet-PCs**

ZAM technische Kurzinformation  
[ZAM-TKI-0376 \(Norton Personal Firewall 2002\)](#)

und interner Bericht  
[ZAM-IB-9916](#)



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

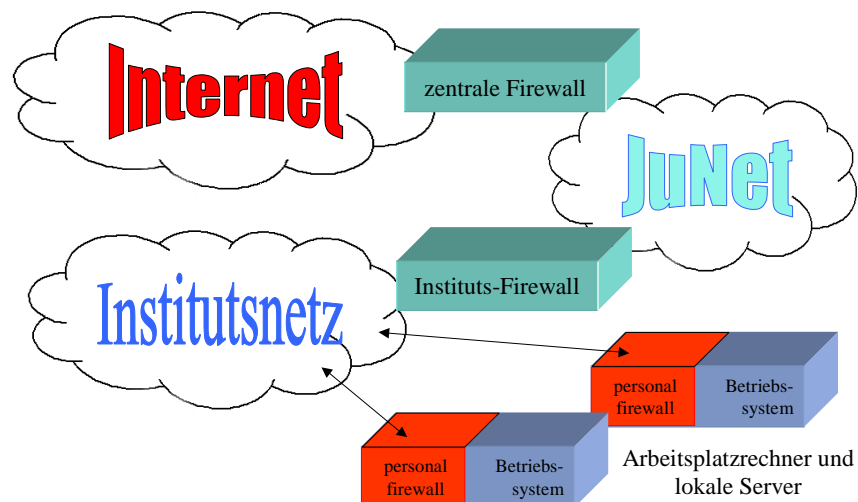


## Funktionen eines IP-Firewalls

- 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>



# ***Symantec Norton Personal Firewall 2002***

**ZAM-TKI-0376**

**Das AtGuard-Nachfolgeprodukt**

**für**

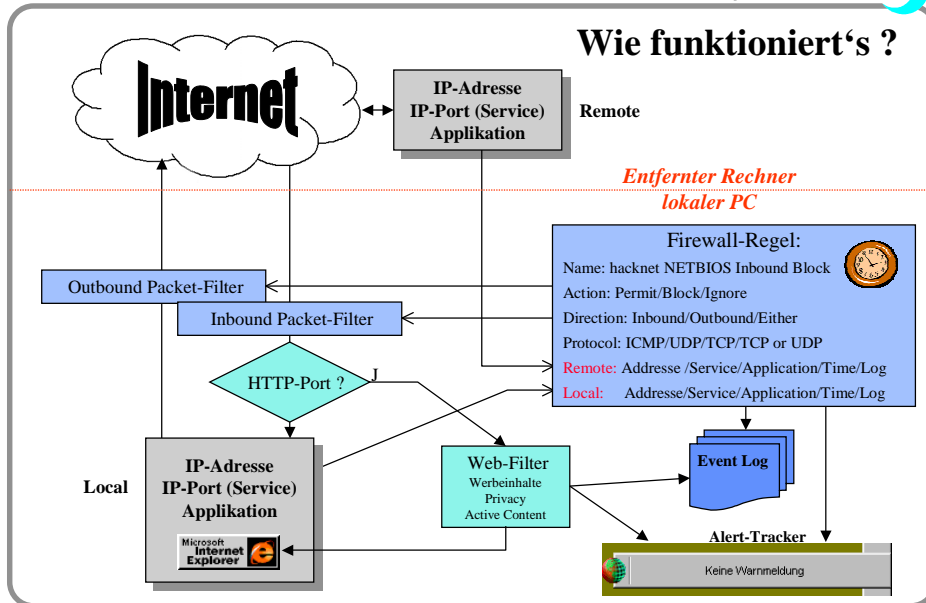
**Windows 95b bis Windows-XP**

**mit (fast) automatischer Selbstkonfiguration**



## **Was ist Symantec Norton Personal Firewall ?**

- 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:
  - Werbeeinhalte (Inbound)
  - Persönliche Benutzerinformationen (Outbound)
  - Aktive, potentiell gefährliche Web-Inhalte (Inbound Scripting, ActiveX, Java)
- Ein Alarmierungswerkzeug für unerwünschte Verbindungsversuche



## Installation von Norton Personal Firewall 2002

- Windows-übliche Installation on-line-Registrierung

**Willkommen Installations-Norton Personal Firewall 2002**

Es wird dringend empfohlen, vor dem Ausführen der Installation alle geöffneten Programme zu schließen.

Klicken Sie auf "Abbrechen", um die Installation zu beenden.

**WARNUNG:** Dieses Programm ist urheberrechtlich geschützt und kann zu erheblichen Schäden führen.

Unberechtigte Reproduktion oder nicht autorisierter Vertrieb dieses Programms oder Teile des Programms werden gerichtlich verfolgt und kann zu erheblichen Schäden führen.

Vielen Dank, dass Sie LiveUpdate verwenden. Folgende Symantec-Produkte sind nun auf dem neuesten Stand:

- Norton Internet Security - Sicherheitsaktualisierungen
- Norton Internet Security - Programmaktualisierungen

LiveUpdate hat 1 Update(s) für dieses Produkt erfolgreich heruntergeladen und installiert. Es wurden alle verfügbaren Updates ausgewählt.

- Automatisches Live-Update der Software über Internet oder [\\pcsrv\public\Symantec](http://pcsrv/public/Symantec)

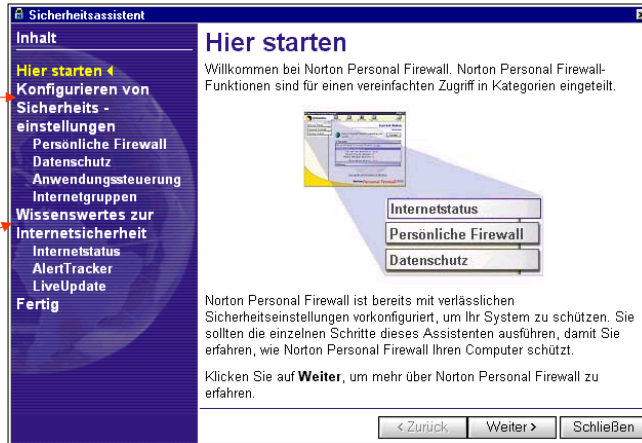


## Konfiguration mit dem Sicherheitsassistenten

- Vereinfachte Einstellung von Firewall (IP-Sicherheit) und Webfiltern (Datenschutz) durch den Sicherheitsassistenten

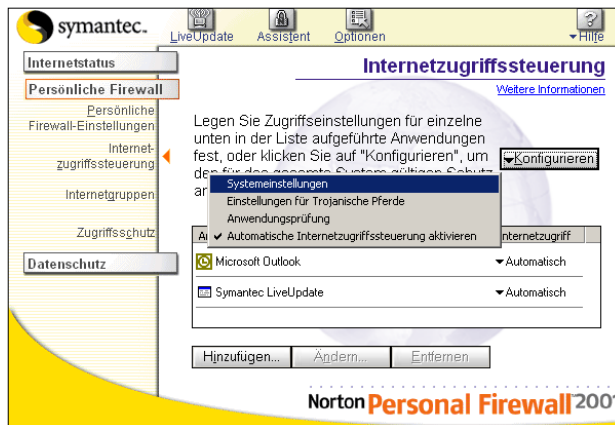
- Konfiguration von Firewall und Webfiltern

- Anzeige von Status und Ereignissen



## Internet-Zugriffssteuerung

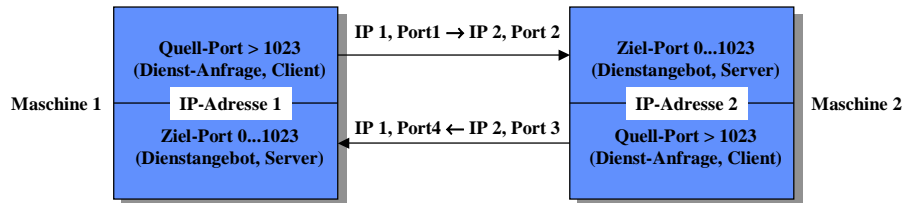
- Systemeinstellungen: Systemweit gültige Firewallregeln für Standardkommunikation
- Einstellungen für Trojanische Pferde: Blockieren und Loggen bekannter Trojaner
- Anwendungsprüfung: Suchen nach Internet-Anwendungen und Zugriffskonfiguration
- Automatische Internet-Zugriffssteuerung aktivieren: Automatische Regelerstellung für unkritische Anwendungen





## 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)



## 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!**



## Standard-Systemdienste und Trojaner

- Vorkonfigurierte Standarddienste (zulassen)

**Einstellungen für Trojanische Pferde**

Die folgenden Optionen werden beim Zugriff auf das Internet in der Reihenfolge zugeordnet.

- Standard Back Office 2000 blockieren**  
Blockieren, Richtung: Ankommend, Computer: Bestimmte, Protokoll: TCP-UDP, Protokolliert als: Sich
- Standard NetBus blockieren**  
Blockieren, Richtung: Ankommend, Computer: Bestimmte, Protokoll: TCP, Protokolliert als: Sich
- Standard GmFriend blockieren**  
Blockieren, Richtung: Ankommend, Computer: Bestimmte, Protokoll: TCP, Protokolliert als: Sich

**Systemeinstellungen**

Die folgenden Optionen werden beim Zugriff auf das Internet in der aufgeführten Reihenfolge zugeordnet.

- Standard Ankommendes ICMP**  
Zulassen, Richtung: Ankommend, Computer: Alle, Kommunikationstypen: Bestimmte, Protokoll: ICMP
- Standard Abgehendes ICMP**  
Zulassen, Richtung: Abgehend, Computer: Alle, Kommunikationstypen: Alle, Protokoll: ICMP
- Standard Ankommendes DIIS**  
Zulassen, Richtung: Ankommend, Computer: Alle, Kommunikationstypen: Bestimmte, Protokoll: UDP

Buttons: Hinzufügen, Ändern, Entfernen, Nach oben, Nach unten, OK, Abbrechen

- und Blockieren/Protokollieren von Trojanern



## Automatische Suche nach Internet-Anwendungen

- Durchsucht das System nach netzwerkfähigen Anwendungen
- Für jede Anwendung läßt sich die Art der zu erstellenden Firewallregel konfigurieren:

- Automatisch
- Alles zulassen
- Alles blockieren
- Interaktive Abfrage, ob zulassen oder nicht

**Anwendungsprüfung**

**Internetzugriffssteuerung**

Die unten aufgelisteten Anwendungen können auf das Internet zugreifen. Sie können eine Anwendung blockieren oder zulassen bzw. Norton Personal Firewall anweisen, eine Anwendung automatisch zu konfigurieren, indem Sie auf die entsprechende Option in der Spalte "Internetzugriff" klicken. Falls Sie sich bei einer Anwendung unsicher sind, entfernen Sie sie aus der Liste. Sie werden dann benachrichtigt, wenn diese Anwendung später versucht, auf das Internet zuzugreifen.

Hi...	Anwendung	Internetzugriff
<input checked="" type="checkbox"/>	Adobe Acrobat 4.0	Abfrage
<input checked="" type="checkbox"/>	Adobe Registration	Automatisch
<input type="checkbox"/>	Beam International Splash! Web Author 1.2	Alle zulassen Alle blockieren Abfrage

Buttons: Hinzufügen..., Ändern..., Entfernen, Alle auswählen, < Zurück, Fertig stellen, Abbrechen



## Internet-Gruppen

- Eintrag einzelner Rechner oder Netze für unbeschränkten Zugriff („Vertraut“) oder für völliges Zugriffsverbot („Eingeschränkt“)

Achtung: keine Alias-Namen verwenden !



## Zugriffsschutz vor Portscans mit Ausnahmen

- Automatisches, 30-minütiges Blockieren externer Adressen, die einen Portscan auf dem lokalen PC durchführen (Hacker-Scan)

- Ausschluß bestimmter Systeme, die legale Scans ausführen, von der Liste der blockierten Systeme



## Die Funktion als Webfilter

- **Datenschutz:** Verhindert die unbeabsichtigte Weitergabe von Benutzerbezogenen Informationen und persönlichen Daten (Mailadresse, Kontonummer etc.) ins Internet (meist an einen Webserver)
- Verhindert das Ablegen von Cookies auf dem Klienten
- **Active Inhalte:** Verhindern der Ausführung potentiell gefährlicher Webinhalte wie Scripting, ActiveX und Java.
- Verwalten individueller Einstellungen für aktive Inhalte für unterschiedliche IP-Domänen und Rechner
- Konfiguration zusätzlicher Webserver-Ports außer dem Standardport 80
- Blockieren von Dauerschleifen für animierte Grafiken (Performance)



## Datenschutzeinstellungen – persönliche Daten

- Filtern vertraulicher Informationen (jedesmal nachfragen)

symantec. LiveUpdate Assistent Optionen

Internetstatus  
Persönliche Firewall  
Datenschutz

**Datenschutz**

Verhindern Sie, dass persönliche Daten, z. B. Kreditkartennummern, Email-Adressen und Cookies, ins Internet übertragen werden.

**Datenschutz aktivieren**

**Benutzerdefinierte Einstellungen**

**Benutzerdef.**

- Klicken Sie zum Ändern der Einstellungen auf "Benutzerdefiniert".
- Um mit den empfohlenen Einstellungen zu arbeiten, klicken Sie auf "Standardstufe".

Vertrauliche Info... Benutzerdefiniert... Standardstufe

**Norton Personal Firewall 2001**

**Datenschutzeinstellungen anpassen**

**Datenschutzeinstellungen anpassen**

[Weitere Informationen](#)

Vertrauliche Informationen

Mittel: Jedes Mal Abfrage einblenden

Cookies

Keine Cookies zulassen (empfohlen)

Browser-Datenschutz aktivieren

Sichere Verbindungen (https) aktivieren

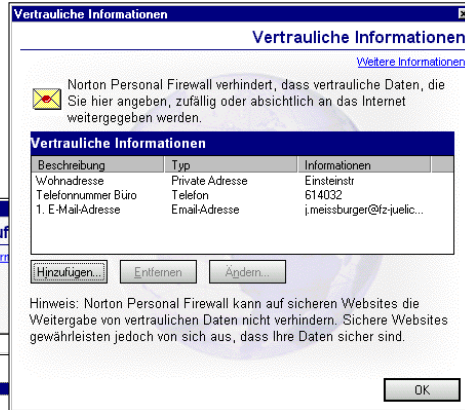
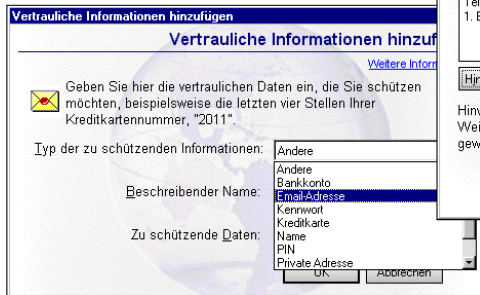
OK Abbrechen

- Cookies und SSL-Verbindungen zulassen



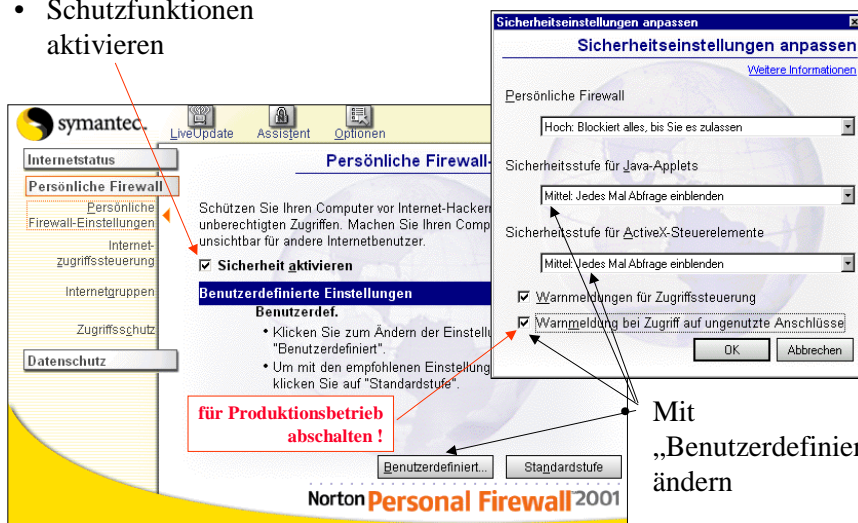
## Datenschutz - Vertrauliche Info

- Schutz sensibler, persönlicher Daten vor der versehentlichen Weitergabe in Webformularen
- Achtung: Kein Schutz bei sicheren SSL-Verbindungen



## Persönliche Firewall-Einstellungen

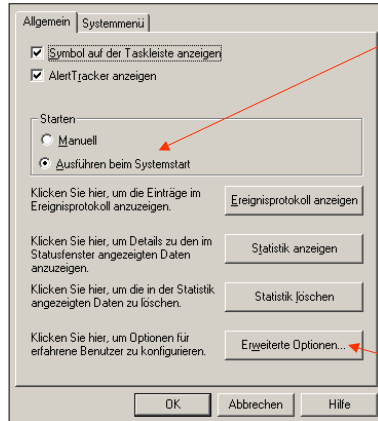
- Schutzfunktionen aktivieren





## Optionen und Erweiterte Optionen

- Start- und Anzeigeeoptionen für Firewall und Alarmanzeige
- Ausführen bei Systemstart aktivieren



- Sicherheitswarnungen werden vom „Alert Tracker“ automatisch auf dem Desktop angezeigt:



- Definition zusätzlicher HTTP-Ports (Web-Dienste)



## Domänenkonzept für Webfilter

**Erweiterte Optionen**

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

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

**Domäne oder Rechner hinzufügen**



## Erweiterte Optionen: Domänen für Webfilter

Spezielle Konfiguration für einzelne Rechner oder IP-Domänen



## Erweiterte Optionen

- Modifikation der Standardeinstellungen für bestimmte Sites oder Domänen wie etwa fz-juelich.de



## Das Ereignisprotokoll

The screenshot shows the Norton Personal Firewall event log. The top window displays messages such as 'Firewall-Konfiguration wurde aktualisiert: 91 Regeln' and 'Eine Instanz von "C:\PROGRAMME\INTERNET EXPLORER...' with timestamps from 03.07.02 15:32:48 to 15:21:57. The bottom window shows a detailed connection log with columns for Datum, Uhrzeit, Benutzer, Remote, Lokal, Gesend. B., Empf. Bytes, and Verst. A specific entry for 03.07.02 15:47:40 shows a connection from 134.94.100.198 to localhost:1027.

**Beispiele:**  
**Firewallregeln**  
**und**  
**Verbindungen**



## Die Verkehrsstatistik

The screenshot displays the Norton Personal Firewall traffic statistics dashboard. It includes several sections:

- Netzwerk-Gesamtraten:** Shows overall network statistics such as 'Gesendete TCP-Bytes: 109997' and 'Empfangene TCP-Bytes: 188806'.
- Webfilter:** Displays statistics for web filtering, including 'Grafiken blockiert' and 'Cookies blockiert'.
- Firewall TCP-Statistik:** Shows TCP connection statistics, including 'Ankommende zugelassen: 3' and 'Abgehende zugelassen: 6'.
- Firewall UDP-Statistik:** Shows UDP connection statistics, including 'Ankommende zugelassen: 0' and 'Abgehende zugelassen: 183'.
- Regelstatistik:** A table showing the status of various firewall rules, including 'Standard Ankommandes...', 'Standard Abgehendes...', and 'Standard Ankommandes...'. Columns include 'Zugel.', 'Blocki.', and 'Werte...'.
- Netzwerkverbindungen:** A table showing active network connections with columns for 'Prot.', 'Progr.', 'Remote', 'Lokal', 'Gese.', 'Empl.', and 'Zeit'.
- Verbindungsstatistik:** A line graph showing the number of connections over time, with a legend for 'HTTP-Verbindungen' and 'HTTP-KB/Sek.'.
- Echtzeitanzeige:** A real-time display area.



## Vergleich zu AtGuard

- Unterstützt im Gegensatz zu AtGuard alle Windows-Versionen (+)
- Ein Überblick über alle Firewallregeln ist nur durch Durchsuchen vieler interaktiver Menüs mit Scrolling möglich (für Experten ungeeignet) (-)
- Der Zugriff von Rechnern und Netzen kann generell über zwei neue Listen „vertraut“ und „eingeschränkt“ geregelt werden (+)
- Der Schutz vor Weitergabe persönlicher Daten (Privacy) wurde durch eine Zeichenketten-basierte Filterfunktion erweitert (+)
- Die Regelerstellung für den Internetzugriff von lokalen Anwendungen auf das Internet (Zugriffssteuerung) kann automatisch erfolgen (+)
- Norton Personal Firewall bietet auch ohne spezielle Konfiguration einen deutlich verbesserten Schutz (+)



## *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
- Regelassistenten 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
- Regelassistent 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“
- Regelassistent abgeschaltet!
- Verwendung numerischer IP-Adressen oder Namensauflösung durch lokale Hosts-Datei (localhost, myclient, myserver....)
- 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, nbssession / 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	adsmprsv.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. Nur so bekommt man wirklich mit, was läuft. Dies betrifft auch die Zugriffssteuerung für Anwendungen!
- 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.
- Regelmäßig Live-Updates ausführen.

