

**Wolfgang Barth**

# **Das Firewall-Buch**

**Grundlagen, Aufbau und Betrieb sicherer  
Netzwerke mit Linux**



# Inhaltsverzeichnis

|   |    |
|---|----|
| <b>1 Ziel dieses Buches</b>             |    |
| <b>2 Wozu braucht man Firewalls?</b>    | 5  |
| 2.1 Der Begriff „Firewall“              | 5  |
| 2.2 Was ein Firewall kann ...           | 6  |
| 2.3 ... und was ein Firewall nicht kann | 7  |
| 2.4 Grundwerte der IT-Sicherheit .      | 8  |
| 2.4.1 Vertraulichkeit                   | 8  |
| 2.4.2 Verfügbarkeit                     | 9  |
| 2.4.3 Integrität                        | 9  |
| 2.5 Zusammenfassung                     | 10 |
| <b>3 Security Policy</b>                | 11 |
| 3.1 Security Policy und Firewalls       | 12 |
| 3.2 Gefährdungspotentiale               | 12 |
| 3.2.1 Externe, aktive Angriffe          | 13 |
| 3.2.2 Interne, aktive Angriffe          | 15 |
| 3.2.3 Autonome Einheiten                | 16 |
| 3.3 Sicherheitspolitik                  | 19 |
| 3.3.1 Sicherheitsziele                  | 19 |
| 3.4 Sicherheitskonzept                  | 24 |
| 3.4.1 Organisatorisches .               | 24 |
| 3.4.2 Infrastruktur .                   | 26 |
| 3.4.3 Einzelne Systeme .                | 27 |

|          |   |           |
|----------|---|-----------|
| 3.4.4    | Netzwerke   | 28        |
| 3.5      | Zusammenfassung                                       | 31        |
| <b>4</b> | <b>Grundlagen des Firewalldesigns</b>                 | <b>33</b> |
| 4.1      | TCP/IP - Netzwerkprotokoll für das Internet           | 34        |
| 4.1.1    | Das OSI-Referenzmodell                                | 34        |
| 4.1.2    | Historische Entwicklung                               | 36        |
| 4.1.3    | DoD-Protokollfamilie (TCP/IP)                         | 37        |
| 4.1.4    | Firewallsysteme und OSI-Ebenen                        | 38        |
| 4.1.5    | IP  | 38        |
| 4.1.6    | TCP   | 40        |
| 4.1.7    | UDP   | 44        |
| 4.1.8    | ICMP  | 45        |
| 4.2      | Paketfilterung  | 45        |
| 4.2.1    | Statische Paketfilterung                              | 47        |
| 4.2.2    | Dynamische Paketfilterung                             | 47        |
| 4.3      | Proxy-Systeme   | 48        |
| 4.4      | Firewallumgebungen                                    | 51        |
| 4.4.1    | Entmilitarisierte Zone: das Grenznetz                 | 51        |
| 4.4.2    | Bastion Hosts   | 52        |
| 4.4.3    | Dual Homed Hosts                                      | 54        |
| 4.5      | Private IP-Adressen                                   | 55        |
| 4.5.1    | Herkömmliche Proxies                                  | 56        |
| 4.6      | Network Address Translation                           | 56        |
| 4.6.1    | IP-Masquerading                                       | 57        |
| 4.6.2    | Transparente Proxies                                  | 58        |
| 4.6.3    | Load Balancing  | 59        |
| 4.7      | Zusammenfassung                                       | 60        |
| <b>5</b> | <b>Paketfilterung und Network Address Translation</b> | <b>61</b> |
| 5.1      | Kernel vorbereiten                                    | 62        |
| 5.2      | Paketfilterung mit iptables                           | 64        |
| 5.2.1    | Ablaufdiagramm des Linux-Kernelfilters                | 64        |

|          |  |            |
|----------|--|------------|
| 5.2.2    | Grundoperationen für Filterregeln            | 65         |
| 5.2.3    | Matching-Optionen für Filterregeln           | 66         |
| 5.2.4    | Targets - Was soll die Filterregel bewirken? | 75         |
| 5.2.5    | Default Policy.                              | 82         |
| 5.2.6    | Regelketten anzeigen, entleeren, überwachen  | 83         |
| 5.2.7    | Weitere Variationen von Filterregeln         | 84         |
| 5.2.8    | Filterregeln testen.                         | 86         |
| 5.2.9    | Filterregeln sichern/restaurieren            | 86         |
| 5.3      | Network Address Translation                  | 87         |
| 5.3.1    | Einsatz von NAT: Schema                      | 88         |
| 5.3.2    | Source-NAT.                                  | 89         |
| 5.3.3    | Destination-NAT.                             | 90         |
| 5.4      | Zusammenfassung                              | 92         |
| 6        | Proxies                                      | 93         |
| 6.1      | SuSE Proxy Suite: ftp-proxy.                 | 95         |
| 6.1.1    | Inbound-Connections.                         | 96         |
| 6.1.2    | Startarten für den ftp-proxy.                | 103        |
| 6.1.3    | Outbound-Connections.                        | 104        |
| 6.1.4    | Transparenter FTP-Proxy.                     | 105        |
| 6.2      | SOCKS.                                       | 106        |
| 6.2.1    | SOCKS V4 im Vergleich zu SOCKS V5            | 107        |
| 6.2.2    | Implementierungen von SOCKS.                 | 108        |
| 6.2.3    | Dante SOCKS-Server.                          | 108        |
| 6.2.4    | Clients mit SOCKS (Socksifying)              | 116        |
| 6.3      | TIS Firewall Toolkit                         | 119        |
| 6.3.1    | Bestandteile des TIS-FWTK.                   | 120        |
| 6.4      | Ausblick                                     | 122        |
| <b>7</b> | <b>Internetdienste und Firewalls</b>         | <b>125</b> |
| 7.1      | Häufig benutzte Internetdienste.             | 126        |
| 7.1.1    | E-Mail: SMTP/POP3.                           | 126        |
| 7.1.2    | Domain Name Service (DNS).                   | 134        |

|          |   |            |
|----------|---|------------|
| 7.1.3    | Terminal-Session: Telnet                          | 142        |
| 7.1.4    | r-Kommandos                                       | 144        |
| 7.1.5    | Secure Shell: sicherer Ersatz für rsh/telnet      | 147        |
| 7.1.6    | File Transfer Protocol (FTP)                      | 153        |
| 7.1.7    | World Wide Web: HTTP                              | 163        |
| 7.1.8    | HTTP via SSL/TLS                                  | 172        |
| 7.1.9    | ping und weitere ICMP-Messages                    | 175        |
| 7.1.10   | Usenet-News: NNTP                                 | 180        |
| 7.1.11   | Zeitsynchronisierung im Netzwerk: NTP             | 183        |
| 7.1.12   | Finger  | 185        |
| 7.1.13   | RPC-Kandidaten: NFS, NIS/YP                       | 186        |
| 7.1.14   | X Window System                                   | 188        |
| 7.2      | Internetdienste starten                           | 189        |
| 7.2.1    | Start als permanenter Daemon                      | 189        |
| 7.2.2    | Start über den inetd-Daemon                       | 190        |
| 7.3      | Internetdienste abschalten                        | 191        |
| 7.3.1    | Start über/sbin/init.d                            | 191        |
| 7.3.2    | Start über inetd                                  | 192        |
| 7.4      | Internetdienste kontrollieren                     | 193        |
| 7.4.1    | Der tcpwrapper                                    | 193        |
| <b>8</b> | <b>Firewalls bauen - einzelner Rechner</b>        | <b>195</b> |
| 8.1      | Absicherung eines einzelnen Rechners              | 195        |
| 8.1.1    | Benutzerverwaltung/Login                          | 196        |
| 8.1.2    | Unnötige Dienste abschalten                       | 198        |
| 8.1.3    | Sichere Konfiguration verbleibender Dienste       | 201        |
| 8.1.4    | Kontrolle über offene Ports                       | 202        |
| 8.2      | Einzelner Rechner mit direktem Internetzugang     | 203        |
| 8.2.1    | Überflüssige Dienste abschalten                   | 204        |
| 8.2.2    | Paketfilterung mit fester IP-Adresse              | 207        |
| 8.2.3    | Skript starten und gesetzte Regeln protokollieren | 223        |
| 8.2.4    | Auswertung der Protokolle                         | 227        |
| 8.2.5    | Dynamische IP-Adressen                            | 232        |

|           |   |            |
|-----------|---|------------|
| 8.2.6     | Variante für dynamische Filterregeln                              | 240        |
| <b>9</b>  | <b>Firewalls bauen - Netzwerk</b>                                 | <b>245</b> |
| 9.1       | Internetzugang über Router/Paketfilter.                           | 245        |
| 9.2       | Einfacher Firewall  | 259        |
| 9.2.1     | Paketfilterung  | 262        |
| 9.2.2     | Proxy-Konfiguration (SOCKS).                                      | 281        |
| 9.2.3     | Caching-Only Nameserver.  | 285        |
| 9.2.4     | Feste IP-Adresse.   | 290        |
| 9.3       | Firewall mit Grenznetz  | 290        |
| 9.3.1     | Paketfilterung  | 292        |
| 9.3.2     | Caching Web-Proxy.  | 306        |
| 9.3.3     | Webserver.  | 308        |
| 9.3.4     | FTP-Server.   | 311        |
| 9.3.5     | Transparente Proxies.   | 316        |
| 9.4       | Ausblicke.  | 318        |
| <b>10</b> | <b>Maintenance: Firewalls installieren, betreiben, überwachen</b> | <b>321</b> |
| 10.1      | Vor der Inbetriebnahme.   | 322        |
| 10.1.1    | Physikalische Sicherheit  | 322        |
| 10.1.2    | Partitionierung/Mounts.   | 324        |
| 10.1.3    | Auswahl der zu installierenden Pakete                             | 326        |
| 10.1.4    | Planung von regelmäßigen Updates                                  | 332        |
| 10.1.5    | Datensicherung, File-Integrity, Worst-Case-Recovery               | 334        |
| 10.2      | Regelmäßige Wartung   | 336        |
| 10.3      | Intrusion Dectection.   | 339        |
| 10.3.1    | Einführung  | 339        |
| 10.3.2    | Snort   | 342        |
| 10.3.3    | Informationsquellen zum Thema IDS                                 | 350        |
| 10.4      | Integritätsprüfung auf Dateiebene.                                | 350        |
| 10.4.1    | Bordmittel: RPM.  | 351        |
| 10.4.2    | Tripwire.   | 353        |
| 10.4.3    | weitere Tools.  | 362        |

# Inhaltsverzeichnis

|          |   |            |
|----------|---|------------|
| 10.5     | Logfile-Überwachung                       | 362        |
| 10.5.1   | syslog                                    | 364        |
| 10.5.2   | logcheck                                  | 369        |
| 10.5.3   | logsurfer                                 | 374        |
| 10.6     | Netzwerkanalyse                           | 390        |
| 10.6.1   | tcpdump                                   | 391        |
| 10.6.2   | ngrep                                     | 397        |
| 10.6.3   | Portscanning: nmap                        | 401        |
| 10.6.4   | Nessus                                    | 407        |
| 10.7     | Port-Überwachung                          | 413        |
| 10.7.1   | scanlogd                                  | 413        |
| 10.7.2   | PortSentry                                | 414        |
| 10.8     | Was tun, wenn es doch passiert ist.       | 415        |
| 10.9     | Zusammenfassung                           | 417        |
| <b>A</b> | <b>TCP/IP: Ausgewählte Kapitel</b>        | <b>419</b> |
| A.1      | IP  | 419        |
| A.2      | TCP                                       | 421        |
| A.3      | UDP                                       | 422        |
| A.4      | ICMP                                      | 422        |
| A.5      | IP Fragmentierung                         | 424        |
| A.6      | ausgewählte TCP/UDP-Portnummern           | 425        |
| <b>B</b> | <b>Runtime-Kernelkonfiguration</b>        | <b>429</b> |
| B.1      | IPForwarding                              | 429        |
| B.2      | IP Spoof Protection                       | 430        |
| B.3      | TCP SYN-Cookies                           | 430        |
| B.4      | ICMPOptions                               | 430        |
| B.5      | Weitere, Device-abhängige Kernelparameter | 431        |
| <b>C</b> | <b>Die Secure Shell: SSH</b>              | <b>433</b> |
| C.1      | Serverinstallation und -konfiguration     | 433        |
| C.1.1    | Hostkey erzeugen                          | 434        |
| C.1.2    | Starten des sshd                          | 434        |

|          |  |     |
|----------|--|-----|
| C.1.3    | Systemweite Konfigurationsdateien                  | 435 |
| C.2      | User-Konfiguration                                 | 437 |
| C.2.1    | Erzeugen des RSA-Schlüssels                        | 437 |
| C.2.2    | Schlüsselverteilung, Logins einrichten             | 438 |
| C.2.3    | Userkonfigurierbare Dateien                        | 439 |
| C.3      | User-Authentifikation mit SSH                      | 441 |
| <b>D</b> | <b>Unterschiede zwischen iptables und ipchains</b> | 445 |
| D.1      | Paket-Routing: Unterschiede                        | 446 |
| D.2      | Änderungen von ipchains auf iptables               | 449 |
| <b>E</b> | <b>Informationsquelle Internet</b>                 | 453 |
| E.1      | SuSE-Linux   | 453 |
| E.2      | Security-Links                                     | 454 |
| E.2.1    | Allgemeine Security-Links                          | 454 |
| E.2.2    | Linux Security-Links                               | 455 |
| E.2.3    | Intrusion Detection                                | 455 |
| E.3      | Verschiedenes                                      | 455 |
| E.3.1    | Linux Online                                       | 455 |
| E.3.2    | Linux und ISDN                                     | 456 |