Disposition

Firewalls unter dem Aspekt von Virtuellen Maschinen

Florian Kogelbauer

2. Februar 2009

Wirtschaftsuniversität Wien

Inhaltsverzeichnis

1. Einleitung

Der nachfolgende Abschnitt soll grundlegende Eigenschaften der vorliegenden Arbeit beschreiben, sowie die damit verbundenen Rahmenbedingungen abklären. Eingangs werden die Zielsetzung der Arbeit, sowie die damit verbundene Forschungsfrage erläutert. Anschließend wird auf die Struktur der Arbeit eingegangen und die Erstellung dieser in einen zeitlichen Rahmen gefasst. Abschließend soll der Zusammenhang zu anderen, von meiner Person, publizierten Arbeiten abgegrenzt werden.

1.1. Zielsetzung

Zielsetzung der Arbeit ist die Darstellung der Besonderheiten, welche bei der Verwendung von Firewalls in Verbindung mit Virtuellen Maschinen auftreten. Darüber hinaus sollen grundlegende Konzepte der Technologien dargestellt werden, als auch die dadurch determinierten Einsatzgebiete. Weiters sollen konkrete Realisierungen, in den entsprechenden Teilbereichen, dargestellt werden und Verbesserungen angesprochen werden.
Zusätzlich soll eine konkrete Softwarelösung – Firewall Builder – in Hinblick auf Virtuelle Maschinen vorgestellt werden. Hierbei soll auf die konkreten Anforderungen sowie die damit verbundenen Problembereiche eingegangen werden. Weiters soll eine experimentelle Erweiterung zur Unterstützung von VMs erstellt, sowie erläutert werden.
Die Dreiteilung der Arbeit soll es ermöglichen, die einzelnen Themenbereiche gesondert, aber auch in Kombination betrachten zu können. Der Leser soll die Möglichkeit erhalten, sich umfassendes Wissen in den unterschiedlichen behandelten Gebieten anzueignen, wobei auf eine konzeptionelle Darstellung geachtet wird, um die Portierbarkeit des Wissens zu ermöglichen.

1.2. Forschungsfrage

Die grundlegende Forschungsfrage dieser Masterarbeit ist die Feststellung von Besonderheiten bei der Verwendung von Firewallsystemen in Verbindung mit Virtuellen Maschinen. Die Feststellung dieser Eigenheiten auf theoretischer Basis als auch die konkrete Realisierung sollen Gegenstand dieser Arbeit sein. Weiters soll untersucht werden, in wie weit die Besonderheiten bei den konkreten Realisierungen berücksichtigt werden können. Die Ausarbeitung diesr Fragestellungen basiert vorwiegend auf folgenden Methoden:

- Literaturrecherche zu den Themengebieten
- Praktische Umsetzung ausgewählter Lösungen und Dokumentation der Ergebnisse

Weiters sollen etwaige Besonderheiten bei der Verbundbildung von Virtuellen Maschinen und dessen Auswirkungen auf Firewalls untersucht werden.

1.3. Thesenstruktur

Um die Zusammenhänge erklären zu können, werden zuvor die Themen Firewalls, als auch das der Virtuellen Maschinen getrennt behandelt. Dies soll dem Leser die Möglichkeit geben, einen Überblick über die Leistungsfähigkeit sowie Zweckmäßigkeit der beiden Technologien zu bekommen. Darüber hinaus werden konkrete Realisierungen dargestellt, welche den Bezug zur Praxis herstellen sollen.
Bezüglich der Firewalls werden, nach allgemeiner Definition (Aufgaben, Abgrenzung, Einsatzgebiete), zuerst grundlegende Netzwerkkenntnisse vermittelt, welche den Leser für sicherheitstechnische Missstände sensibilsieren sollen. Darüber hinaus werden klassische Angriffe und Angriffsmethoden erläutert. Weiters soll der Einsatz von Firewalltechnologie zur Vermeidung bzw. Unterbindung dieser Angriffe dargestellt werden. Danach wird auf die unterschiedlichen Konzepte der Firewalls eingegangen und eine konkrete Realisierung (Packetfilter mittels iptables) vorgestellt. Abschließend wird erläutert, welche Angriffe auf Firewallsysteme es gibt und wie diese erkannt werden können.
Bezüglich der Virtuellen Maschinen werden, nach allgemeiner Definition, die Aufgaben, sowie die geschichtliche Entwicklung dargestellt. Anschließend wird auf die unterschiedlichen Virtualisierungstechniken eingegangen. Weiters werden die Konzepte des Bridgings als auch der Virtuellen Netzwerkadapter erläutert, welcher im Abschnitt der gemeinsamen Nutzung besondere Bedeutung zukommen. Darüber hinaus sollen Kriterien für die sinnvolle Auswahl von Virtualisierungsprodukten dargestellt und erläutert werden.

Danach werden konkrete Virtualisierungslösungen vorgestellt und auf die sicherheitstechnischen Fragen eingegangen.
Im letzten Abschnitt der Arbeit wird der kombinierte Einsatz der zuvor vorgestellten Technologien dargestellt. Zu Beginn werden die speziellen Anforderungen, welche an Firewalls unter Virtuellen Maschinen gestellt werden, dargestellt. Anschießend wird der Einsatz von Firewalls im VM-Verbund und der damit verbundenen Besondereheiten betrachtet. Abschließend soll eine konkrete Lösung zur Erstellung von Firewall Policies vorgestellt werden. In diesem Zusammenhang soll untersucht werden, ob eine hinreichende Unterstützung für Virtuelle Maschinen und der damit verbundenen virtuellen Netzwerkadapter gegeben ist. Weiters werden konkrete Erweiterungen dargestellt und eine experimentelle Realisierung vorgestellt.

1.4. Zeitplan

Als zeitlicher Rahmen für die Erstellung dieser Arbeit soll eine Semesterlänge herangezogen werden. Zur einfacheren Überprüfung der Leistungserstellung, sowie des -fortschritts werden Meilensteine sowie zugehörige Stichtage vorgeschlagen. Der Zeitplan inklusive des Meilensteinplans sieht dann wie folgt aus:

NUMMER	MEILENSTEIN – BESCHREIBUNG	DATUM
1	**Start – Bearbeitung** (Beginn der Ausarbeitungsphase)	01.02.2009
2	**Abschluss Kapitel: Firewalls** (Fertigstellung des Kapitels Firewalls - Grundlagen, Theorie, Anwendung)	15.03.2009
3	**Abschluss Kapitel: Virtuelle Maschinen** (Fertigstellung des Kapitels Virtuelle Maschinen - Grundlagen, Theorie, Anwendung)	30.04.2009
4	**Abschluss Kapitel: Firewalls unter dem Aspekt der Virtuellen Maschinen** (Fertigstellung des Kapitels Firewalls unter dem Aspekt der Virtuellen Maschinen - Kombination, Anwendung, Realisierungsgrad, Unterstützung, aktuelle Entwicklungen u. Trends	15.06.2009
5	**Ende – Bearbeitung** (Ende der Ausarbeitungsphase - Abgabe der Arbeit)	30.06.2009

Tabelle 1.1.: Meilensteinplan als zeitliches Referenzsystem

Die verbleibende Zeit zwischen der Fertigstellung des letzten Kapitels und der Fertigstellung der Arbeit soll als Puffer für etwaige Änderungen bzw. Verbesserungen dienen. Ansonsten sind die Bearbeitungszeiten pro Kapitel mit der Arbeitzeit von eineinhalb Monaten geplant.

1.5. Abgrenzung zu anderen publizierten Arbeiten

Die Abgrenzung bezieht sich im Speziellen auf die bereits veröffentlichten Bakkalaureatsarbeiten des Autors, wovon eine in Zusammenarbeit mit einem, hier nicht explizit genannten Unternehmen erarbeitet wurde. Die zweite Arbeit stellt eine theoretische Ausarbeitung eines sicherheitstechnischen Themas dar.[Kog07, Kog08]

Bezüglich der Bakkalaureatsarbeit [Kog07][1], welche in Zusammenarbeit mit einem Unternehmen eine praktische Realisierung eines Softwaremoduls darstellt, ist keinerlei Überschneidung festzustellen. Die darin behandelten Themen der Erstellung eines Softwaremoduls für die Dokumentenverteilung an die Kunden, als auch die Verzeichnisdienste (insb. OpenLDAP) werden daher ausgegrenzt.

Bei der Bakkalaureatsarbeit [Kog08][2] hingegen sind auf Grund der Themenverwandtschaft (Sicherheitstechnik und grundlegende Netzwerkstrukturen) Überschneidungen festzustellen. Im Speziellen betrifft dies die Grundlagen der Netzwerktechnik, als auch die darin definierten Referenzmodelle [Kog08, S. 6–21]. Basierend auf diesen Grundlagen wird eine Vertiefung bis hin zur Bit–(Sequenz)Ebene angestrebt, welche als Grundlage für das Filtern bzw. den Einsatz von Firewalls verstanden werden kann.

Bei der Thematik der Virtuellen Maschinen ist keine Themenverwandtschaft zu den bisher publizierten Arbeiten festzustellen, weshalb eine klare Abgrenzung leicht möglich ist.

[1] [Kog07]
Kogelbauer, Florian: *Elektronische Dokumentenverwaltung und -bereitstellung auf einer Website durch Implementierung eines Zusatzmoduls DokuSERVE.* Wirtschaftsuniversität Wien, 2007.

[2] [Kog08]
Kogelbauer, Florian: *Virtual Private Networks - Grundlagen, Geschichte sowie aktuelle Entwicklungen.* Wirtschaftsuniversität Wien, 2008.

Teil I.

Firewalls

2. Firewall - Grundlagen

Grundidee hinter dem Firewall Gedanken – wozu dient sie grob vereinfacht – Versinnbildlichung des Konzepts – Sensibilisierung des Lesers für das Sicherheitskonzept – Definitionszitat – [FG05, WP07, Jan07]

2.1. Aufgaben der Firewall

Wozu dienen Firewalls im Konkreten, was sind ihre Aufgabe – wer benötigt sie – Ziele, die durch den Einsatz erreicht werden sollen – [Spe06, Les06, FG05]

2.2. Abgrenzung der Aufgaben von Firewalls

Was zählt nicht zu den Aufgaben von Firewalls – was können diese nicht – Abgrenzung der Thematik – [Les06]

2.3. Einsatzbereiche

Gebiete in denen Firewalls Verwendung finden – von Personal Firewall bis zum Unternehmensnetzwerk – [FG05, Les06]

3. Grundlagen der Netzwerktechnik

Übersicht, der zur Datenvermittlung im Internet notwendigen Protokolle und Dienste – sowie Darstellung ihrer Schwächen – Grundlage für die Darstellung, wie Firewalls Daten kontrollieren und gegebenenfalls verwerfen und abändern – [Tan02]

3.1. TCP / IP Modell

Überblick über die Funktionalität – Schwächen – möglicherweise kurze Gegenüberstellung zum ISO/OSI Referenzmodell – Darstellung der Daten(Paket)kapselung – [Tan02]

3.2. Internet Protocol (IP)

Funktionsüberblick – Verwendung – Aspekte in Verbindung mit Firewalls (Verwerfen von IP-Adressen aus dem Bereich 10.x.x.x u.ä.) – [Tan02, Spe06, Les06]

3.3. Transmission Control Protocol (TCM)

Funktionsüberblick – Verwendung – Aspekte in Verbindung mit Firewalls (Staffelung bzw. Reihenfolge der Kontrollbefehle – z.B. Paket mit gesetztem SYN-Bit aber ohne ACK-Bit entspricht vermutlich einem Verbindungsaufbau u.ä.) – [Tan02, Spe06, Les06]

3.4. User Datagram Protocol (UDP)

Funktionsüberblick – Verwendung – Aspekte in Verbindung mit Firewalls (Spezialfälle, wo keine Antwort abgewartet wird u.ä.) – [Tan02, Spe06, Les06]

3.5. Adress Resulution Protocol (ARP)

Funktionsüberblick – Verwendung – Aspekte in Verbindung mit Firewalls (Sniffer – veränderbare MAC–Adressen – Promiscuous Mode u.ä.) – [Tan02, Spe06, Les06]

3.6. Internet Control Message Protocol (ICMP)

Funktionsüberblick – Verwendung – Fehler- und Kontrollnachrichtenüberblick – [Tan02, Spe06, Les06]

3.7. Domain Name Service (DNS)

Funktionsüberblick – Verwendung – Aspekte in Verbindung mit Firewalls (Port 53 UDP oder TCP damit Verwendung möglich u.ä.) – [Tan02, Spe06, Les06]

4. Angriffe u. Angriffsarten

Grundbegriffe und -techniken für die mutwillige Ausnützung von Schwachstellen sollen erläutert werden – die Verwendung von Firewalls zur Unterbindung soll erläutert werden (sofern sinnvoll und möglich) – [Tan02, WP07, Spe06, Les06, Jan07]

4.1. Denial-of-Service (DoS) Attacken

4.1.1. DoS mittels Flooding

4.1.2. DoS mittels ICMP

4.2. Cracking

4.3. Würmer und Trojaner

4.4. Schädliche Inhalte in HTML-Seiten

4.5. Sonstige

Angriffe auf die Privatsphäre, Social Engineering, u.ä. – kurzer Überblick, dass die zuvor genannten Techniken nicht vollständig sind – ständig werden neue Methoden entwickelt – [Gra01, Fyo98, Fyo97, Erb01]

5. Firewallgrundkonzepte

Dieser Abschnitt behandelt Konzepte, wie Firewalls ausgelegt bzw. implementiert werden können. Zusätzlich zu den beiden Grundkonzepten der Filter und Proxies werden auch Praktiken wie NAT (Network Address Translation) und kombinierte Konzepte erläutert.

5.1. Filter (Paketfilter)

Aufbau – Funktionsweise – Nutzen – [Spe06, Les06, Gre00]

5.2. Proxies

Aufbau – Funktionsweise – Nutzen – [Spe06, Les06, Gre00]

5.3. Network Address Translation (NAT)

Aufbau – Funktionsweise – Nutzen – [Les06, Tan02]

5.4. Kombinationen

Screened Hosts und Screened Subnets werden hier erläutert – [Les06]

6. Realisierungsbeispiele

Die nachfolgenden Beispiele konzentrieren sich ausschließlich auf Realisierungen die auf Linux Distributionen aufsetzen. Durch die Vielzahl der verfügbaren Distributionen wird auf eine konzeptuelle Darstellung (zwecks Portierbarkeit) geachtet.

6.1. (Paket-)filter mit iptables

Erklären der Grundidee – Aufbau darstellen – einführende Beispiele (z.B. die absolut sichere Firewall) – (roter Faden zur später vorgestellten Software – Firewall Builder) – [Les06, Spe06]

6.2. pf unter OpenBSD

Erklären der Grundidee – Aufbau darstellen – Installation – einführende Beispiele – [Ope09]

7. Exkurs: Angriffe und deren Erkennung auf Firewalls

Darstellung aktueller Techniken zur Erkennung – Möglichkeiten zur Früherkennung – Grenzen der Techniken und deren Einsatz – [Gla07, Rue07]

Teil II.

Virtuelle Maschinen

8. Virtuelle Maschinen - Grundlagen

Die nachfolgenden Kapitel sollen über die Grundlagen sowie die Funktionalität von Virtuellen Maschinen (nachfolgend kurz VMs) Aufschluss geben. Darüber hinaus werden die geschichtliche Entwicklung, als auch die zugrunde liegenden Techniken beschrieben. Weiters werden das Thema des Bridgings als auch mögliche Kriterien für die richtige Auswahl von Lösungen beschrieben.

8.1. Aufgaben der Virtuellen Maschinen

Was stellen VMs zur Verfügung – wo liegt der Sinn bzw. die Vorteile – [Tho08, Fis08a]

8.2. Geschichtliche Entwicklung

Aus welcher Notwendigkeit hat sich die Virtualisierung entwickelt – womit hat es begonnen (Hardwarevirtualisierung) – [Tho08, Fis08b, Xen08]

8.3. Einsatzbereiche und -gründe

Wo finden die VMs Anwendung – typische Einsatzbereiche mit Begründung – [Tho08]

8.4. Virtualisierungstechniken

Welche Arten von Virtualisierungstechniken gibt es – wie werden sie unterschieden – Vor- u. Nachteile – Zweckmäßigkeit – [Tho08, Fis08b, Xen08, QEM08, Vir08, Fis08a]

8.4.1. Hardware-Virtualisierung

8.4.2. Para-Visualisierung

8.4.3. Virtualisierung auf Kernel-Ebene

8.4.4. Virtualisierung auf einem Wirt-System

8.5. Bridging und Co.

Grundlagen des Bridgings – Virtuelle Netzwerkadapter u.ä. – als Basis sollen Linux Distributionen dienen – [Tan02, Tho08, Fis08b, Xen08, QEM08, Vir08, Fis08a]

8.6. Kriterien für die Auswahl

Kriterien die bei der Auswahl berücksichtigt werden – [Tho08]

9. Virtualisierungslösungen

Im nachfolgendem Kapitel werden konkrete Virtualisierungslösungen vorgestellt. Bei der Auswahl wurde auf die Aktualität, als auch auf die Verbreitung Rücksicht genommen – möglicherweise verfügbare Benchmark-Ergebnisse

9.1. Xen

Grundlagen – Geschichte – Leistungsumfang – dahinterstehende Technik – [Fis08b, Xen08, Fis08a]

9.1.1. Grundlagen

9.1.2. Geschichte

9.1.3. Leistungsumfang

9.1.4. Technik

9.2. KVM

Grundlagen – Geschichte – Leistungsumfang – dahinterstehende Technik – [QEM08, Fis08a, PW07]

9.2.1. Grundlagen

9.2.2. Geschichte

9.2.3. Leistungsumfang

9.2.4. Technik

9.3. VirtualBox

Grundlagen – Geschichte – Leistungsumfang – dahinterstehende Technik – [Vir08, Fis08a]

9.3.1. Grundlagen

9.3.2. Geschichte

9.3.3. Leistungsumfang

9.3.4. Technik

9.4. Sonstige

Beschreibung von nicht zuvor genannten VM-Lösungen – auch auf Windows Betriebssystemen – [Tho08] – aber auch andere Online-Ressourcen

10. VM-Sicherheit

10.1. Wechselwirkung Host- und Gastmaschine

Grundlagen über die VM-Sicherheit – Unterscheidung auf Hostsystem und VM-System (von den vorgestellten Lösungen) – [Rad08, Her08, Bab08, Bro08, Won08]

10.2. Exkurs: Hardwarevirtualisierungsbefehle

Virtualisierungsbefehle der CPUs (aktuelle Befehle - sowie mögliche damit verbundene Gefahrenquellen) – [Int08, AMD07]

Teil III.

Firewalls unter dem Aspekt der Virtuellen Maschinen

11. Firewalls unter VMs

Erläuterung zusätzlicher Bedingungen, wenn Firewalls in Verbindung mit VMs eingesetzt werden – Einsatz auf Host- u. Clientseite – kohärente Konfiguration auf den Systemen – Firewalls und virtuelle Netzwerkadapter – [Fis08a, PW07, Bro08, Cum08, Dub08, Gre08]

12. Firewalls und VM-Clusters

Art der Vernetzungen – VPNs (SSL) – Zusammenhänge zwischen der Firewallkonfiguration und dem Verbund von Virtuellen Maschinen – Dienstefreigaben (Ports) – iptables-Beispiele – [Lip07, Fis08a, PW07]

13. Firewall Policies mit dem FirewallBuilder

Beschreibung des Firewall Builders – [Kur08]

13.1. Grundlagen

13.2. Geschichte

13.3. Verwendung

13.4. Unterstützung von VMs

13.5. Problembereiche

13.6. Erweiterung des Firewall Builders

Literaturverzeichnis

[AMD07] AMD: *IOMMU Architectural Specification*, 2007. `http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/34434.pdf`, Abruf am 2009-02-02.

[Bab08] Babcock, Charles: *Virtualization's Tipping Point.* InformationWeek, (1186):14, Mai 2008.

[Bro08] Brodkin, Jon: *VMware partners demonstrate VMsafe virtual security prototypes.* Network World (Online), September 2008.

[Cum08] Cummings, Joanne: *How to segregate virtual servers.* Network World, 25(11):40, März 2008.

[Dub08] Dubie, Denise: *Vendors tackle virtual security.* Network World, 25(36):20, September 2008.

[Erb01] Erb, Hubert: *Die Cyberspace-Fallen des FBI*, 2001. `http://www.heise.de/tp/r4/artikel/7/7634/1.html`, Abruf am 2008-12-30.

[FG05] Fritsch, Jörg und Steffen Gundel: *Firewalls im Unternehmenseinsatz: Grundlagen, Betrieb und Produkte.* Dpunkt Verlag, 2. überarb. und aktualis. a. Auflage, August 2005.

[Fis08a] Fischer, Marcus: *Ubuntu GNU/Linux: Aktuell zu "Hardy Heron".* Galileo Press, 3., aktualisierte a. Auflage, Juni 2008. `http://openbook.galileocomputing.de/ubuntu/`.

[Fis08b] Fischer, Marcus: *Xen: Von den Grundlagen bis zur Administration.* Galileo Press, 1. Auflage, November 2008.

[Fyo97] Fyodor: *Port Scanning Techniques*, 1997. `http://nmap.org/book/man-port-scanning-techniques.html`, Abruf am 2008-12-30.

[Fyo98] Fyodor: *Remote OS detection via TCP/IP Stack FingerPrinting.* Phrack Magazine(8), 1998. `http://www.phrack.org/issues.html?issue=54&id=9#article`, Abruf am 2008-12-30.

[Gla07] Gladewitz, Robert: *Angriffserkennung in Firewalls: Implementierung einer schwellwertbasierten Net- und Portscananalyse.* Vdm Verlag Dr. Müller, 1. Auflage, Juli 2007.

[Gra01] Granger, Sarah: *Social Engineering Fundamentals, Part I: Hacker Tactics*, 2001. `http://www.securityfocus.com/infocus/1527`, Abruf am 2008-12-30.

[Gre00] Grennan, Mark: *Firewall and Proxy Server HOWTO*, 2000. `http://www.grennan.com/Firewall-HOWTO.html`, Abruf am 2008-12-30.

[Gre08] Greene, Tim: *10 security threats to watch for.* Network World, 25(15):30, April 2008.

[Her08] Hernick, Joe: *Securing VMware.* InformationWeek, (1193):31, Juli 2008.

[Int08] Intel: *Intel(r) VT for Direct IO*, 2008. `http://download.intel.com/technology/computing/vptech/Intel(r)_VT_for_Direct_IO.pdf`, Abruf am 2009-02-02.

[Jan07] Janowicz, Krzysztof: *Sicherheit im Internet.* O'Reilly, 3. Auflage, Juli 2007. `http://www.oreilly.de/german/freebooks/sii3ger/`.

[Kog07] Kogelbauer, Florian: *Elektronische Dokumentenverwaltung und -bereitstellung auf einer Website durch Implementierung eines Zusatzmoduls DokuSERVE.* Wirtschaftsuniversität Wien, 2007.

[Kog08] Kogelbauer, Florian: *Virtual Private Networks - Grundlagen, Geschichte sowie aktuelle Entwicklungen.* Wirtschaftsuniversität Wien, 2008.

[Kur08] Kurland, Vadim: *Firewall Builder FAQ*, Juli 2008. `http://www.fwbuilder.org/docs/firewall_builder_faq.html`, Abruf am 2008-12-30.

[Les06] Lessig, Andreas G.: *Linux Firewalls- Ein praktischer Einstieg.* O'Reilly, 2. aufl. Auflage, 2006.

[Lip07] Lipp, Manfred: *VPN - Virtuelle Private Netzwerke: Aufbau und Sicherheit.* Addison-Wesley, München, 1. Auflage, September 2007.

[Ope09] OpenBSD: *PF: Der OpenBSD Packet Filter*, 2009. `http://openbsd.org/faq/pf/de/index.html`, Abruf am 2009-02-02.

[PW07] Plötner, Johannes und Steffen Wendzel: *Linux: Das distributionsunabhängige Handbuch*. Galileo Press, 1. auflage. Auflage, Oktober 2007. `http://openbook.galileocomputing.de/linux/`.

[QEM08] QEMU: *QEMU Emulator User Documentation*, Jänner 2008. `http://bellard.org/qemu/qemu-doc.html`, Abruf am 2008-12-30.

[Rad08] Radcliff, Deb: *HOW TO ROOT OUT ROOTKITS*. Network World, 25(31):28, August 2008.

[Rue07] Ruef, Marc: *Die Kunst des Penetration Testing - Handbuch für professionelle Hacker: Sicherheitslücken finden, Gefahrenquellen schließen*. C & l Computer- U. Literaturverlag, 1. auflage Auflage, Juni 2007.

[Rus00] Russell, Rusty: *Linux IP Firewalling Chains*, 2000. `http://people.netfilter.org/~rusty/ipchains/`, Abruf am 2008-12-30.

[Spe06] Spenneberg, Ralf: *Linux-Firewalls mit iptables & Co*. Addison-Wesley, München, 1. Auflage, 2006.

[Spe07] Spenneberg, Ralf: *Sicherheit für virtuelle Systeme mit Xen*, Februar 2007. `http://www.linux-magazin.de/videos/sicherheit_fuer_virtuelle_systeme_mit_xen`, Abruf am 2008-12-30.

[Tan02] Tanenbaum, Andrew S.: *Computer Networks*. Prentice Hall International, 4. a. (International edition). Auflage, August 2002.

[Tho08] Thorns, Fabian: *Das Virtualisierungs-Buch*. C & l Computer- U. Literaturverlag, 2., aktualisierte und erweiterte auflage. Auflage, September 2008.

[Vir08] VirtualBox: *Sun xVM VirtualBox - User Manual*, Dezember 2008. `http://dlc-cdn-rd.sun.com/c1/virtualbox/2.1.0/UserManual.pdf?e=1230900701&h=59dd6233e80ec9b7ad2a52666075bc07`, Abruf am 2008-12-30.

[Won08] Wong, Bill: *Will Virtualization Save The Day?* Electronic Design, 56(9):47, Mai 2008.

[WP07] Wendzel, Steffen und Johannes Plötner: *Netzwerk-Sicherheit: Risikoanalyse, Methoden und Umsetzung*. Galileo Press, 2., aktualis. und erw. a. Auflage, Februar 2007.

[Xen08] Xen: *Xen v3.3 - Users' Manual*, 2008. `http://bits.xensource.com/Xen/docs/user.pdf`, Abruf am 2008-12-30.