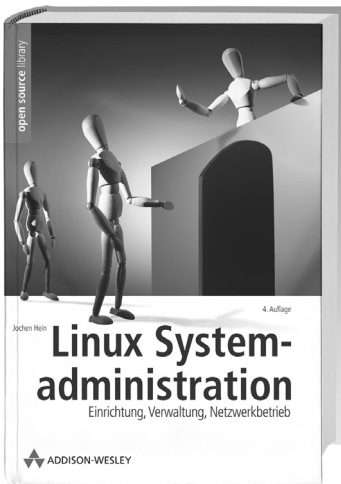


VPN mit Linux

open source library

Open Source Software wird gegenüber kommerziellen Lösungen immer wichtiger. Addison-Wesley trägt dieser Entwicklung Rechnung mit den Büchern der **Open Source Library**. Administratoren, Entwickler und User erhalten hier professionelles Know-how, um freie Software effizient einzusetzen. Behandelt werden sowohl Themen wie Betriebssysteme, Netzwerke und Sicherheit als auch Programmierung.

Eine Auswahl aus unserem Programm:



Linux für den fortgeschrittenen Systemadministrator, der lernt, wie man Linux bei verteilten Netzumgebungen einsetzt. Die vierte Auflage wurde durchgehend überarbeitet, aktualisiert und erweitert. Wesentliche Neuerungen betreffen Linux-Standards, XML-Tools, Internet-Zugang mit DSL, VPNs, BIND9/dnssec.

Linux-Systemadministration
Jochen Hein
643 Seiten
EUR 49,95 [D], sFr 77,50
ISBN 3-8273-1992-7



Sicherheit ist ein Problem aller Betriebssysteme, und meist ist es teuer, eine Installation wirklich sicher zu machen. In diesem Buch zeigt der Autor, dass dies auch ohne einen größeren finanziellen Aufwand möglich ist. Hier erfahren Sie, wie Sie Linux mit Hilfe von Open-Source-Tools wie z.B. LIDS, Snort, NMap, Webmin oder Nessus sicher machen.

Linux Security
Josef Brunner
518 Seiten
EUR 49,95 [D], 51,40 [A]
ISBN 3-8273-1999-4

Ralf Spenneberg

VPN mit Linux

**Grundlagen und Anwendung
Virtueller Privater Netzwerke mit Open Source-Tools**



ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Hardware- und Softwarebezeichnungen, die in diesem Buch erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen oder sollten als solche betrachtet werden.

Umwelthinweis:
Dieses Produkt wurde auf chlorfrei gebleichtem Papier gedruckt.

06 05 04

ISBN 3-8273-2114-X

© 2004 by Addison-Wesley Verlag,
ein Imprint der Pearson Education Deutschland GmbH
Martin-Kollar-Straße 10–12, D-81829 München/Germany
Alle Rechte vorbehalten
Einbandgestaltung: Marco Lindenbeck (mlindenbeck@webwo.de)
Fachliche Redaktion: Wilhelm Dolle, Berlin
Lektorat: Boris Karnikowski, bkarnikowski@pearson.de
Korrektorat: Bettina Bläß, Köln
Herstellung: Philipp Burkart, pburkart@pearson.de
Satz: reemers publishing services gmbh, Krefeld, www.reemers.de
Druck: Bercker, Kevelaer
Printed in Germany

Für Claudia

Inhaltsverzeichnis

Vorwort	11
Teil I Grundlagen	13
1 Einleitung	15
1.1 Was ist ein Virtuelles Privates Netzwerk?	15
1.2 Aufgaben eines VPN	16
1.3 Vor- und Nachteile eines VPN	33
1.4 Open-Source und Sicherheit	38
1.5 Kommerzielle Lösungen	42
1.6 Verschiedene VPN Szenarien	46
2 Kryptografie	53
2.1 Einleitung	53
2.2 Geschichte	54
2.3 Symmetrische Verschlüsselung	57
2.4 Cipher Block Chaining (CBC)	63
2.5 Asymmetrische Verschlüsselung	64
2.6 Hash-Funktion	73
3 VPN Protokolle	77
3.1 Einleitung	77
3.2 IPsec	79
3.3 L2TP	104
4 Keymanagement	109
4.1 Einleitung	109
4.2 X.509 Zertifikat	113
4.3 Public Key Infrastruktur – PKI	116
4.4 Smartcard	117

Teil II Praktische Umsetzung	119
5 FreeS/WAN	121
5.1 Einleitung	121
5.2 Lizenz	122
5.3 Installation	122
5.4 FreeS/WAN Komponenten	138
5.5 Konfiguration von FreeS/WAN	139
5.6 FreeS/WAN 2.x	228
5.7 Konfiguration der Firewall	231
6 IPsec mit Linux 2.6	237
6.1 Einleitung	237
6.2 Lizenz	238
6.3 Installation	238
6.4 Konfiguration mit setkey und racoon	240
6.5 Verwendung von isakmpd	274
7 Aufbau heterogener Virtueller Privater Netze	297
7.1 Einleitung	297
7.2 Interoperabilitätsprobleme	298
7.3 Microsoft Windows 98/Me/NT	298
7.4 Microsoft Windows 2000 und Windows XP	299
7.5 Checkpoint Firewall-1 NG	308
7.6 Cisco	309
8 Aufbau einer Public Key Infrastruktur	311
8.1 Einleitung	311
8.2 TinyCA	312
8.3 XCA	319
8.4 OpenCA	327

Teil III Fortgeschrittene Konfiguration und Fehlersuche	329
9 Fortgeschrittene Konfiguration	331
9.1 Aufbau einer Verbindung mit dynamischen IP Adressen auf beiden Seiten.	331
9.2 Advanced Routing	333
9.3 Quality of Service	335
9.4 Nicht-IP-Tunnel	339
9.5 NAT Traversal	345
9.6 DHCP-over-IPsec	346
9.7 Opportunistische Verschlüsselung	354
9.8 Einsatz von Hardware Kryptoprozessoren	361
9.9 Automatisches Laden der CRL	362
9.10 Hochverfügbarkeit	364
9.11 Smartcard Unterstützung	368
10 Fehlersuche	379
10.1 Werkzeuge	379
10.2 Typische Fehler und ihre Ursachen	382
11 Testumgebungen	387
11.1 Testumgebungen	387
11.2 Physikalische Testumgebungen	389
11.3 VMware	389
11.4 User-Mode-Linux	390
A Lizenzen	395
B Die CD ROM zum Buch	403
C Glossar	405
D Bibliografie	409
Stichwortverzeichnis	411

Vorwort

Dieses Buch versucht den Aufbau von Virtuellen Privaten Netzwerken (VPN) mit Linux zu beschreiben. Dabei sollen dem Anwender die verschiedenen unter Linux zur Verfügung stehenden Werkzeuge und Vorgehensweisen nahe gebracht werden. Um einen Einsatz in heterogenen Netzwerken zu ermöglichen, beschränkt sich das Buch jedoch auf die anerkannte und seit Jahren im Einsatz befindliche Protokollfamilie IPsec. Es wird vorausgesetzt, dass Sie mit Linux oder einem anderen kommerziellen UNIX Derivat grundsätzlich vertraut sind. Außerdem werden grundlegende Netzwerkkennnisse erwartet.

Das Buch ist in mehrere Teile gegliedert:

- Grundlagen
- Praktische Umsetzung
- Fortgeschrittene Konfiguration und Fehlersuche

Teil 1 *Grundlagen* beginnt mit einer allgemeinen Einführung in die Technik und Grundlagen Virtueller Privater Netzwerke. Anschließend werden die verschiedenen Verschlüsselungsalgorithmen, die hier zum Einsatz kommen erklärt. Ihre Kenntnis ist bei der Anwendung eines VPN nicht zwingend notwendig, jedoch erlaubt ein gewisses Grundwissen eine Einschätzung ihrer Sicherheit.

Schließlich werden die eingesetzten Protokolle der IPsec Familie betrachtet und analysiert. Auch dieses Wissen ist nicht zwingend erforderlich für einen Betrieb eines VPNs. Bei einer Fehlersuche ist dieses Hintergrundwissen jedoch sehr nützlich, wenn nicht sogar obligatorisch.

Sollte das entsprechende Grundwissen bereits vorhanden sein, oder Sie ungeduldig mit dem Aufbau eines VPNs beginnen wollen, so können Sie direkt mit Teil 2 des Buches beginnen. Für das Verständnis, die Planung und die Fehlersuche empfiehlt es sich jedoch zu einem späteren Zeitpunkt Teil 1 nachzulesen.

Teil 2 *Praktische Umsetzung* beschreibt den Aufbau einfacher Virtueller Privater Netzwerke mit den momentan zur Verfügung stehenden Implementierungen für den Linux Kernel 2.4 und 2.6, FreeS/WAN, racoon und isakmpd. Hierbei werden die Konfigurationsparameter beschrieben und einfache VPN Lösungen aufgebaut.

Teil 3 *Fortgeschrittene Konfiguration und Fehlersuche* beschreibt besondere Eigenheiten der Implementierungen und stellt zusätzliche Funktionalitäten vor, die für die eine oder andere Implementierung einzigartig sind. Hier werden Funktionen besprochen, wie NAT Traversal, DHCP-over-IPsec und opportunistische Verschlüsselung. Auch die Unterstützung von Hardware Kryptoprozessoren zur Beschleunigung der Verschlüsselung wird hier angesprochen.

In Teil 3 werden auch die wichtigsten Werkzeuge zur Fehlersuche vorgestellt. Außerdem enthält dieser Teil auch die häufigsten Fehlermeldungen und ihre wahrscheinlichsten Ursachen.

Bei der Strukturierung des Buches habe ich versucht, die Aufgabenstellungen bei Aufbau eines VPNs in Schritt für Schritt Anleitungen durch zusprechen. Sicherlich wird dabei nicht jedes Problem geklärt. Um diesem Missstand Rechnung zu tragen, behandelt Teil 3 komplizierte und besondere Fragestellungen. Hierbei ist es jedoch nur möglich Einblicke in bestimmte Probleme zu geben. Sie sollen als Anregung aufgefasst werden und den Lösungsweg aufzeigen.

Beim Schreiben des Buches waren behilflich: Fridtjof Busse, Wilhelm Dolle und Thomas Walpuski. Diesen Personen möchte ich hierfür danken.

Alles in allem hoffe ich, dass mir ein Buch gelungen ist, mit dem Sie in der Lage sind, den Einsatz von Virtuellen Privaten Netzwerken auf der Basis von Linux abzuwägen und umzusetzen. Schließlich bleibt mir nur, Ihnen dabei Spaß und viel Erfolg zu wünschen.

Kontakt für Rückfragen und Anmerkungen

Virtuelle Private Netzwerke sind ein sehr aktuelles Thema. Dies führt dazu, dass die entsprechenden Technologien und Produkte ständig weiterentwickelt werden. Die in diesem Buch besprochenen Themen sind dabei sicherlich keine Ausnahme. Wenn Sie also zum Inhalt dieses Buches Updates, Korrekturen oder einfach Anregungen loswerden möchten, können Sie mich unter ralf.spenneberg@mut.de erreichen. Sofern es das Volumen zulässt, bin ich auch gerne bereit Fragen zum Thema zu beantworten. Unabhängig davon werde ich versuchen unter <http://www.spenneberg.com/> Updates und Korrekturen zum Buch zu veröffentlichen.