

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

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

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