

# Inhaltsübersicht

Vorwort zur 2. Auflage . . . . .	23
<b>Teil I Grundlagen</b>	<b>27</b>
Einleitung . . . . .	29
1 Was ist ein virtuelles privates Netzwerk? . . . . .	31
2 Aufgaben eines VPN . . . . .	33
3 Schutz durch ein VPN . . . . .	41
4 Open-Source und Sicherheit . . . . .	55
5 Kommerzielle Lösungen . . . . .	59
6 Verschiedene VPN-Szenarien . . . . .	63
7 Kryptografie . . . . .	69
8 VPN-Protokolle . . . . .	89
<b>Teil II Praktische Umsetzung</b>	<b>121</b>
9 IPsec mit dem Linux-Kernel 2.6 . . . . .	123
10 Manuell verschlüsselte Verbindung . . . . .	133
11 Openswan und strongSwan . . . . .	143
12 Konfiguration von Openswan und strongSwan . . . . .	151
13 Automatische Verbindung mit dem Pluto-IKE-Daemon . . . . .	173
14 Roadwarrior . . . . .	199

# INHALTSÜBERSICHT

15	Konfiguration der Firewall . . . . .	213
16	Automatische Verbindung mit racoon . . . . .	219
17	OpenBSD lsakmpd . . . . .	247
18	Aufbau heterogener virtueller privater Netze . . . . .	267
<b>Teil III IKEv2 mit strongSwan</b>		<b>285</b>
19	Verbindungen mit PreShared Keys . . . . .	287
20	Datei strongswan.conf . . . . .	293
21	Verbindungen mit Zertifikaten . . . . .	301
22	Hybrid-Modus . . . . .	303
23	Configuration Payload . . . . .	307
24	Das strongSwan Network-Manager-Plug-In . . . . .	311
25	Windows 7 und IKEv2 . . . . .	313
26	Hochverfügbarkeit mit strongSwan . . . . .	319
<b>Teil IV Fortgeschrittene Konfiguration und Fehlersuche</b>		<b>327</b>
27	Keymanagement . . . . .	329
28	Aufbau einer Public-Key-Infrastruktur . . . . .	337
29	Firewalling der IPsec-Verbindungen mit IPtables . . . . .	353
30	Aufbau einer Verbindung mit dynamischen IP-Adressen auf beiden Seiten . . . . .	357
31	Advanced Routing . . . . .	359

# INHALTSÜBERSICHT

32	Nicht-IP-Tunnel . . . . .	361
33	NAT-Traversal . . . . .	367
34	XAuth und IKE-Config-Mode . . . . .	369
35	Kerberos . . . . .	381
36	Opportunistische Verschlüsselung . . . . .	383
37	Einsatz von Hardware-Kryptoprozessoren . . . . .	391
38	Prüfung der Zertifikate . . . . .	395
39	Dead Peer Detection . . . . .	399
40	Hochverfügbarkeit . . . . .	401
41	Smartcard-Unterstützung . . . . .	405
42	DMVPN . . . . .	413
43	Fehlersuche . . . . .	417
44	Testumgebungen . . . . .	421

## Teil V OpenVPN 2.x 427

45	Einführung . . . . .	429
46	Ein einfacher Tunnel . . . . .	433
47	Zertifikate . . . . .	445
48	Verteilung von IP-Adressen . . . . .	457
49	Zusätzliche Netze . . . . .	465
50	Fortgeschrittene Funktionen . . . . .	469

## INHALTSÜBERSICHT

51	OpenVPN-Management-Schnittstelle . . . . .	485
52	Anmeldung mit Benutzername/Kennwort . . . . .	487
53	Smartcards . . . . .	489
54	OpenVPN auf Windows . . . . .	493
55	Grafische Oberflächen . . . . .	499
<b>Teil VI Anhang</b>		<b>505</b>
	Die CD-ROM zum Buch . . . . .	507
	Literaturverzeichnis . . . . .	509
	Stichwortverzeichnis . . . . .	511

# Inhaltsverzeichnis

<b>Vorwort zur 2. Auflage</b>	23
<b>I Grundlagen</b>	27
<b>Einleitung</b>	29
<b>1 Was ist ein virtuelles privates Netzwerk?</b>	31
<b>2 Aufgaben eines VPN</b>	33
2.1 Gefahren im Internet	33
2.2 Schutz durch eine Firewall	35
2.3 Paketfilter	35
2.4 Proxy-Firewall	37
2.5 Zusammenfassung	39
<b>3 Schutz durch ein VPN</b>	41
3.1 Authentifizierung	41
3.2 Vertraulichkeit	46
3.3 Integrität	47
3.4 Vor- und Nachteile eines VPN	48
3.5 VPNs und Firewalls	50
<b>4 Open-Source und Sicherheit</b>	55
<b>5 Kommerzielle Lösungen</b>	59
5.1 Cisco	59
5.2 Checkpoint FW-1/VPN-1	59
5.3 Microsoft Windows	60
5.4 Microsoft Windows 98/ME/NT	60
5.5 SSH Sentinel	61
5.6 GreenBow-VPN-Client	61
5.7 SafeNet SoftRemote	61
5.8 OpenBSD, FreeBSD, NetBSD	62
5.9 Weitere Produkte	62

# INHALTSVERZEICHNIS

<b>6</b>	<b>Verschiedene VPN-Szenarien</b>	63
6.1	Kommunikation zwischen zwei Netzwerken	63
6.2	Kommunikation zwischen zwei Rechnern	63
6.3	Kommunikation zwischen vielen festen Standorten	64
6.4	Anbindung von Telearbeitsplätzen an einen Standort	65
6.5	Anbindung von Außendienstmitarbeitern (Roadwarriors) an einen Standort	66
6.6	Absicherung eines Wireless LAN	67
6.7	Opportunistische Verschlüsselung	67
<b>7</b>	<b>Kryptografie</b>	69
7.1	Einleitung	69
7.2	Geschichte	70
7.3	Symmetrische Verschlüsselung	73
7.3.1	Data Encryption Standard (DES)	75
7.3.2	3DES	75
7.4	International Data Encryption Algorithm (IDEA)	76
7.4.1	RC4/RC5/RC6	76
7.4.2	Blowfish	76
7.4.3	Twofish	77
7.4.4	AES	77
7.4.5	Weitere Verfahren	78
7.4.6	Cipher Block Chaining (CBC)	78
7.5	Asymmetrische Verschlüsselung	78
7.6	Das Beste aus beiden Welten	80
7.7	Public-Key-Schlüssellängen	82
7.8	RSA	82
7.9	ElGamal	83
7.10	Digital Signature Algorithm (DSA)	83
7.11	Diffie-Hellman	83
7.12	Hash-Funktion	86
7.13	MD5	87
7.14	SHA	88
<b>8</b>	<b>VPN-Protokolle</b>	89
8.1	Einleitung	89
8.2	IPsec	90
8.3	Integrität und Authentifizierung bei IPsec	91

# INHALTSVERZEICHNIS

8.4	Verschlüsselung bei IPsec . . . . .	92
8.5	Anti-Replay-Schutz . . . . .	93
8.6	Tunnel- und Transportmodus . . . . .	94
8.7	Authentication Header – AH . . . . .	95
8.8	Encapsulated Security Payload – ESP . . . . .	97
8.9	Security Association . . . . .	99
8.10	Security Policy . . . . .	100
8.11	Internet Key Exchange – IKEv1 . . . . .	100
8.11.1	Der Main-Modus . . . . .	101
8.11.2	Der Aggressive-Modus . . . . .	105
8.11.3	Der Quick-Modus . . . . .	106
8.11.4	UDP Encapsulation . . . . .	106
8.11.5	DHCP-over-IPsec . . . . .	109
8.12	IKEv2 . . . . .	111
8.12.1	Überblick . . . . .	112
8.12.2	IKEv2 im Detail . . . . .	113
8.12.3	CREATE_CHILD_SA-Nachrichten . . . . .	115
8.12.4	INFORMATIONAL-Nachrichten . . . . .	116
8.12.5	Cookies . . . . .	116
8.12.6	Implementierungen . . . . .	117
8.13	L2TP . . . . .	118
<b>II</b>	<b>Praktische Umsetzung</b>	<b>121</b>
<b>9</b>	<b>IPsec mit dem Linux-Kernel 2.6</b> . . . . .	<b>123</b>
9.1	Geschichte . . . . .	123
9.2	Lizenz . . . . .	124
9.3	Installation . . . . .	124
9.3.1	Kernel . . . . .	124
9.4	Userspace-Befehle . . . . .	127
9.5	Konfiguration . . . . .	127
9.6	Das Kommando setkey . . . . .	128
<b>10</b>	<b>Manuell verschlüsselte Verbindung</b> . . . . .	<b>133</b>
10.1	Manuelle Verbindung im Transportmodus . . . . .	133
10.2	Manuelle Verbindung im Tunnelmodus . . . . .	137

# INHALTSVERZEICHNIS

10.3	Erweiterungen und Anmerkungen	138
10.4	Fazit	141
<b>11</b>	<b>Openswan und strongSwan</b>	<b>143</b>
11.1	Hintergründe	143
11.2	Lizenz	144
11.3	Installation von Openswan	144
11.3.1	Kompilierung und Installation des Sourcecodes	144
11.4	Installation von strongSwan	146
11.4.1	Kompilierung und Installation des Sourcecodes	146
11.5	Openswan-Komponenten	150
11.6	StrongSwan-Komponenten	150
<b>12</b>	<b>Konfiguration von Openswan und strongSwan</b>	<b>151</b>
12.1	Allgemeine Konfigurationsparameter	151
12.1.1	ipsec.secrets	152
12.2	ipsec.conf	155
12.3	Setup-Parameter	156
12.4	Verbindungsparameter	157
12.5	Allgemeine Parameter	157
12.6	Der Kommandozeilenbefehl ipsec	160
12.6.1	Openswan ipsec	161
12.6.2	strongSwan-IPsec-Starter: ipsec	169
<b>13</b>	<b>Automatische Verbindung mit dem Pluto-IKE-Daemon</b>	<b>173</b>
13.1	Konfiguration	174
13.1.1	Authentifizierung mit PreShared Keys (PSK)	174
13.2	Aufbau des Tunnels	176
13.3	Verbesserungen und Erweiterungen	178
13.4	Fazit	180
13.5	Automatisch verschlüsselte Verbindung mit X.509-Zertifikaten	180
13.5.1	Erzeugung von X.509-Zertifikaten mit OpenSSL	181
13.5.2	Anpassungen in der Konfiguration	186
13.5.3	Aufbau des Tunnels	188
13.6	Verbesserungen und Erweiterungen	192
13.7	Erweiterte Nutzung der Zertifikate bei strongSwan	194
13.7.1	Zertifikate mit Wildcards	194

# INHALTSVERZEICHNIS

13.7.2	Nutzung der CA-Zertifikate für Tunnel . . . . .	195
13.7.3	X.509-Attribute . . . . .	196
13.8	Fazit . . . . .	197
<b>14</b>	<b>Roadwarrior</b> . . . . .	199
14.1	Roadwarrior mit PreShared Key (PSK) . . . . .	200
14.1.1	VPN-Gateway . . . . .	201
14.1.2	Roadwarrior-Konfiguration . . . . .	203
14.1.3	Roadwarrior in Aggressive-Modus . . . . .	204
14.1.4	Fazit . . . . .	205
14.2	Roadwarrior mit X.509-Zertifikaten . . . . .	206
14.2.1	VPN-Gateway . . . . .	206
14.2.2	Roadwarrior . . . . .	208
14.2.3	Fazit . . . . .	211
<b>15</b>	<b>Konfiguration der Firewall</b> . . . . .	213
15.1	Nutzung von leftfirewall und rightfirewall . . . . .	215
15.2	Anpassung des _updown-Scripts . . . . .	216
15.3	Fazit . . . . .	218
<b>16</b>	<b>Automatische Verbindung mit racoon</b> . . . . .	219
16.1	Konfiguration von racoon . . . . .	219
16.1.1	Start von Racoon . . . . .	219
16.1.2	Racoon-Konfigurationsdatei . . . . .	222
16.1.3	Steuerung mit racoonctl . . . . .	233
16.2	Verbindungen mit PreShared Keys . . . . .	233
16.3	Fazit . . . . .	239
16.4	Racoon und X.509-Zertifikate . . . . .	239
16.5	Racoon und Roadwarriors . . . . .	243
16.6	Racoon als Roadwarrior . . . . .	245
<b>17</b>	<b>OpenBSD Isakmpd</b> . . . . .	247
17.1	Installation . . . . .	247
17.2	Anwendung mit PSKs . . . . .	248
17.3	Die Konfigurationsdatei isakmpd.conf . . . . .	248
17.4	Die Richtliniendatei isakmpd.policy . . . . .	254
17.5	Start und Test der Verbindung . . . . .	255
17.6	Anwendung mit einem X.509-Zertifikat . . . . .	257

# INHALTSVERZEICHNIS

17.7	Die Konfigurationsdatei <code>isakmpd.conf</code>	258
17.8	Die Richtliniendatei <code>isakmpd.policy</code>	260
17.9	Die Erzeugung und Speicherung der X.509-Zertifikate	261
17.10	Roadwarriors und der <code>Isakmpd</code>	262
17.11	Aggressive-Modus und PSKs	264
17.12	IKE-Config-Mode	265
17.13	Fazit	265
<b>18</b>	<b>Aufbau heterogener virtueller privater Netze</b>	<b>267</b>
18.1	Einleitung	267
18.2	Interoperabilitätsprobleme	268
18.3	Microsoft Windows XP, Windows Vista und Windows 7	268
18.3.1	Markus Müllers <code>ipsec.exe</code>	270
18.4	Shrew Soft VPN Client	275
18.5	Checkpoint Firewall-1 NG	282
18.6	Cisco	283
<b>III</b>	<b>IKEv2 mit strongSwan</b>	<b>285</b>
<b>19</b>	<b>Verbindungen mit PreShared Keys</b>	<b>287</b>
19.1	PSKs und Roadwarriors	289
19.2	Mob-IKE	290
19.3	Narrowing der Traffic-Selektoren	290
<b>20</b>	<b>Datei <code>strongswan.conf</code></b>	<b>293</b>
20.1	Charon	293
20.2	Protokollierung	296
20.3	<code>libstrongswan</code>	296
20.4	Manager	297
20.5	Mediator	298
20.6	OpenAC	298
20.7	Pluto	298
20.8	IP-Adressen-Pools	299
20.9	<code>SCEPClient</code>	299
<b>21</b>	<b>Verbindungen mit Zertifikaten</b>	<b>301</b>
21.1	Nutzung von URLs zur Übertragung der Zertifikate	301

# INHALTSVERZEICHNIS

<b>22 Hybrid-Modus</b> . . . . .	303
22.1 Radius . . . . .	305
<b>23 Configuration Payload</b> . . . . .	307
<b>24 Das strongSwan Network-Manager-Plug-In</b> . . . . .	311
<b>25 Windows 7 und IKEv2</b> . . . . .	313
<b>26 Hochverfügbarkeit mit strongSwan</b> . . . . .	319
26.1 Das Problem der Synchronisation . . . . .	319
26.2 Mögliche Lösungen . . . . .	319
26.3 strongSwan-Ansatz . . . . .	320
26.4 ClusterIP . . . . .	322
26.5 Konfiguration . . . . .	324
<b>IV Fortgeschrittene Konfiguration und Fehlersuche</b> . . . . .	327
<b>27 Keymanagement</b> . . . . .	329
27.1 Einleitung . . . . .	329
27.2 Zufallszahlen . . . . .	329
27.3 Lebensdauer von Schlüsseln . . . . .	330
27.4 Kennwörter und symmetrische Schlüssel . . . . .	331
27.5 Öffentliche Schlüssel . . . . .	331
27.6 X.509-Zertifikate . . . . .	332
27.7 Aufbau eines X.509-Zertifikats . . . . .	333
27.8 Public-Key-Infrastruktur – PKI . . . . .	335
27.9 Smartcard . . . . .	336
<b>28 Aufbau einer Public-Key-Infrastruktur</b> . . . . .	337
28.1 Einleitung . . . . .	337
28.1.1 Certificate Authority . . . . .	337
28.1.2 Registration Authority . . . . .	338
28.1.3 Directory Service . . . . .	338
28.2 TinyCA . . . . .	338
28.2.1 Installation . . . . .	339
28.2.2 Aufbau einer CA mit TinyCA . . . . .	339
28.2.3 Export der Zertifikate . . . . .	341

# INHALTSVERZEICHNIS

28.3	XCA	344
28.3.1	Installation	344
28.3.2	Anwendung von XCA	344
28.3.3	Migration einer CA zum XCA-Werkzeug	348
28.4	OpenCA	348
<b>29</b>	<b>Firewalling der IPsec-Verbindungen mit IPtables</b>	<b>353</b>
<b>30</b>	<b>Aufbau einer Verbindung mit dynamischen IP-Adressen auf beiden Seiten</b>	<b>357</b>
<b>31</b>	<b>Advanced Routing</b>	<b>359</b>
31.1	Gateway-Routing	359
<b>32</b>	<b>Nicht-IP-Tunnel</b>	<b>361</b>
32.1	GRE	361
32.2	L2TP	362
<b>33</b>	<b>NAT-Traversal</b>	<b>367</b>
33.1	Alternative NAT-Konfiguration	367
<b>34</b>	<b>XAuth und IKE-Config-Mode</b>	<b>369</b>
34.1	DHCP-over-IPsec	369
34.2	XAuth	369
34.2.1	strongSwan	370
34.2.2	Openswan	370
34.2.3	Racoon	372
34.3	IKE-Config-Mode	374
34.3.1	Openswan	374
34.3.2	strongSwan	375
34.3.3	Racoon	376
34.3.4	lsakmpd	379
<b>35</b>	<b>Kerberos</b>	<b>381</b>
<b>36</b>	<b>Opportunistische Verschlüsselung</b>	<b>383</b>
36.1	Funktionsweise	384
36.2	OE-Initiator	384
36.3	Volle opportunistische Verschlüsselung	385
36.4	OE-Gateway	386

# INHALTSVERZEICHNIS

36.5 Test der opportunistischen Verschlüsselung . . . . .	387
36.6 Policy-Gruppen . . . . .	388
<b>37 Einsatz von Hardware-Kryptoprozessoren . . . . .</b>	<b>391</b>
37.1 VIA Padlock . . . . .	391
37.2 OpenBSD Crypto Framework . . . . .	391
<b>38 Prüfung der Zertifikate . . . . .</b>	<b>395</b>
38.1 Automatisches Laden der CRL . . . . .	395
38.1.1 Racoon und lsakmpd . . . . .	396
38.2 Online Certificate Status Protocol (OCSP) . . . . .	396
<b>39 Dead Peer Detection . . . . .</b>	<b>399</b>
<b>40 Hochverfügbarkeit . . . . .</b>	<b>401</b>
<b>41 Smartcard-Unterstützung . . . . .</b>	<b>405</b>
41.1 Installation . . . . .	405
41.1.1 Installation von OpenCT . . . . .	405
41.1.2 Installation von PCSC-Lite . . . . .	406
41.1.3 Installation von OpenSC . . . . .	406
41.2 Installation von Openswan und strongSwan . . . . .	406
41.3 Konfiguration des Lesegerätes und der Karte . . . . .	406
41.3.1 Anwendung in strongSwan . . . . .	411
<b>42 DMVPN . . . . .</b>	<b>413</b>
42.1 NHRP . . . . .	414
42.2 OpenNHRP . . . . .	414
<b>43 Fehlersuche . . . . .</b>	<b>417</b>
43.1 *swan-Debugging . . . . .	417
43.2 Debugging bei Racoon . . . . .	418
43.2.1 Racoon-Fehlermeldungen . . . . .	418
43.3 Debugging beim lsakmpd . . . . .	419
43.4 Weitere Werkzeuge für das Debugging . . . . .	419
<b>44 Testumgebungen . . . . .</b>	<b>421</b>
44.1 Testumgebung I . . . . .	422
44.2 Testumgebung II . . . . .	422
44.3 Physikalische Testumgebungen . . . . .	423

# INHALTSVERZEICHNIS

44.4	VMware	423
44.5	KVM	424
44.6	Aufbau virtueller Netzwerke	424
<b>V</b>	<b>OpenVPN 2.x</b>	<b>427</b>
<b>45</b>	<b>Einführung</b>	<b>429</b>
45.1	Betriebssysteme	429
45.2	Aufbau	430
<b>46</b>	<b>Ein einfacher Tunnel</b>	<b>433</b>
46.1	Installation von OpenVPN 2.x	433
46.1.1	Manuelle Installation	433
46.1.2	OpenSUSE-RPM	435
46.1.3	Fedora-RPM	436
46.1.4	Debian und Ubuntu	436
46.2	Konfiguration von OpenVPN	436
46.3	Warum sollten Sie diesen Tunnel nicht verwenden?	442
<b>47</b>	<b>Zertifikate</b>	<b>445</b>
47.1	Easy-RSA	445
47.1.1	Variablendefinition	445
47.1.2	Zertifikatsautonität	447
47.1.3	Zertifikate für Server und Clients	448
47.1.4	Widerruf von Zertifikaten	450
47.1.5	Diffie-Hellman-Parameter	451
47.2	Verteilung der Schlüssel	452
47.3	Konfigurationsanpassungen	452
<b>48</b>	<b>Verteilung von IP-Adressen</b>	<b>457</b>
48.1	Serverkonfiguration	457
48.2	Client-Konfiguration	458
48.3	Weitere Clients	459
48.4	Weitere Optionen	460
48.5	Änderung des Default-Gateways	461
48.6	Feste Zuweisung von IP-Adressen	462

# INHALTSVERZEICHNIS

<b>49 Zusätzliche Netze</b> . . . . .	465
49.1 Zusätzliche Netze auf der Seite des Servers . . . . .	465
49.2 Zusätzliche Netze auf der Seite des Clients . . . . .	466
49.3 Kommunikation der Clients untereinander . . . . .	467
<b>50 Fortgeschrittene Funktionen</b> . . . . .	469
50.1 Sicherheit . . . . .	469
50.1.1 Wechsel des Benutzerkontextes . . . . .	469
50.1.2 Betrieb ohne jedes Root-Privileg . . . . .	470
50.1.3 Chroot . . . . .	471
50.1.4 Schlüssellängen . . . . .	472
50.1.5 Einsatz von Hardware-Beschleunigung . . . . .	473
50.1.6 Signatur der Pakete . . . . .	473
50.2 Verfügbarkeit . . . . .	474
50.3 TCP und Proxies . . . . .	476
50.3.1 TCP . . . . .	476
50.3.2 Proxy . . . . .	477
50.3.3 Gemeinsame Portnutzung mit einem Webserver . . . . .	478
50.4 OpenVPN im Bridge-Modus . . . . .	478
50.4.1 Windows . . . . .	479
50.5 Lastverteilung und Hochverfügbarkeit . . . . .	481
50.6 Quality of Service (QoS) . . . . .	483
<b>51 OpenVPN-Management-Schnittstelle</b> . . . . .	485
<b>52 Anmeldung mit Benutzername/Kennwort</b> . . . . .	487
52.1 Verzicht auf Client-Zertifikate . . . . .	488
<b>53 Smartcards</b> . . . . .	489
53.1 PKCS#11 . . . . .	490
53.2 Anpassungen in OpenVPN . . . . .	491
53.3 Microsoft CryptoAPI . . . . .	491
<b>54 OpenVPN auf Windows</b> . . . . .	493
54.1 Installation . . . . .	493
54.1.1 Windows 7 . . . . .	494
54.2 Erzeugung eines eigenen Installationsprogramms . . . . .	495

## INHALTSVERZEICHNIS

<b>55</b>	<b>Grafische Oberflächen</b>	499
55.1	OpenVPN Management Tool	499
55.2	OpenVPN-GUI	500
55.3	OpenVPN-Admin	502
55.4	KVpnc	502
55.5	Tunnelblick	503
<b>VI</b>	<b>Anhang</b>	<b>505</b>
	<b>Die CD-ROM zum Buch</b>	507
	<b>Literaturverzeichnis</b>	509
	<b>Stichwortverzeichnis</b>	511