

Dirk Becker

OpenVPN

Das Praxisbuch

Auf einen Blick

1	Einführung	17
2	Netzwerkgrundlagen	41
3	Software	87
4	Authentisierung und Verschlüsselungsarten	105
5	OpenVPN konfigurieren	135
6	Plugins	189
7	Weitere Konfigurationen	193
8	Tipps	219
9	Fehlersuche und Probleme	237
10	Optionen	247
11	Skripte	283

Inhalt

Vorwort	11
---------------	----

1 Einführung 17

1.1	VPN (Virtual Private Network)	18
1.2	Alternativen zu einem VPN	21
1.2.1	Telnet	22
1.2.2	File Transfer Protocol – FTP	23
1.2.3	Secure Shell – SSH	24
1.2.4	Sonstige	25
1.3	IPSec, FreeS/WAN & Co.	26
1.3.1	Internet Protocol Security – IPSec	26
1.3.2	FreeS/WAN, Openswan und strongSwan	27
1.4	OpenVPN	28
1.4.1	Informationen zu OpenVPN	28
1.4.2	Verschlüsselung bei OpenVPN	29
1.4.3	Verbindungsarten	30
1.4.4	Sonstiges	31
1.5	Szenario	32
1.5.1	Hintergründe	33
1.5.2	Netzwerkdaten	35
1.6	Weitere Dokumentationen	38
1.7	Newsgroups	39

2 Netzwerkgrundlagen 41

2.1	ISO/OSI-Schichtenmodell	42
2.2	Topologien	46
2.3	Ethernet	52
2.4	LAN & WAN	54
2.5	Protokolle	55
2.6	TCP/IP – das Internetprotokoll	58
2.6.1	DoD-Schichtenmodell	58
2.6.2	IP (Internet Protocol)	60
2.6.3	TCP (Transmission Control Protocol)	64
2.6.4	UDP (User Datagram Protocol)	65
2.6.5	DNS (Domain Name System)	66
2.6.6	Routing	69
2.7	WLAN	71

2.8	Sicherheit im Netzwerk	75
2.9	Netzwerktools und Diagnose	77
2.9.1	ifconfig/ipconfig	77
2.9.2	ping	78
2.9.3	nslookup	79
2.9.4	netio	80
2.10	Einrichtung	81
2.10.1	Windows	82
2.10.2	Linux	83
2.10.3	Apple	84
2.11	Sonstiges	85

3 Software 87

3.1	OpenVPN	88
3.1.1	Installation unter Linux	88
3.1.2	Installation unter Windows	92
3.1.3	Installation unter Mac OS X	95
3.2	bridge-utils	95
3.2.1	Installation unter Linux	95
3.2.2	Installation unter Windows	96
3.3	OpenSSL	97
3.3.1	Installation unter Linux	97
3.3.2	Cygwin – OpenSSL unter Windows	98
3.4	Grafische Oberflächen	100
3.4.1	OpenVPN GUI für Windows	100
3.4.2	OpenVPN Control	101
3.4.3	OpenVPN-Admin	101
3.4.4	Tunnelblick für Mac OS X	102
3.4.5	Viscosity	102
3.5	Sonstiges	102
3.5.1	Weitere Quellen	103
3.5.2	Virtuelle Maschinen	103

4 Authentisierung und Verschlüsselungsarten 105

4.1	SSL/TLS	106
4.1.1	Authentisierung	108
4.1.2	Schlüsselaustausch	108
4.1.3	Verschlüsselung	108
4.1.4	Sonstiges	108

4.2	Symmetrische Verschlüsselung (statischer Schlüssel)	109
4.3	Asymmetrische Verschlüsselung (zertifikatbasiert)	113
4.3.1	Digitale Zertifikate	113
4.3.2	Ablauf bei Verwendung eines Zertifikates	115
4.3.3	Ablauf bei der Erstellung eines Zertifikates	116
4.4	Zertifizierungsstelle mit OpenSSL	117
4.4.1	Eigene Zertifizierungsstelle (Certification Authority)	117
4.4.2	Zertifikate erstellen	121
4.4.3	Zertifikate zusammenfassen (PKCS#12)	122
4.4.4	Zertifikate übergeben	123
4.4.5	Zertifikatssperrliste (Certificate Revocation List – CRL)	124
4.5	Zertifikate mit OpenVPN – Easy-RSA	126
4.5.1	Mini-Zertifizierungsstelle	127
4.5.2	Zertifikate erstellen	129
4.5.3	Zertifikate übergeben	130
4.5.4	Zertifikate im PKCS#12-Format	130
4.5.5	Zertifikate sperren	131
4.6	Zertifikate mit einer GUI	131
4.7	Zusammenfassung	132
4.7.1	Statischer Schlüssel	132
4.7.2	Zertifikate	133

5 OpenVPN konfigurieren 135

5.1	Netzwerkschnittstellen	136
5.1.1	Punkt-zu-Punkt-Verbindungen	137
5.1.2	Multi-Client-Verbindungen	138
5.2	Firewall und Routing	138
5.2.1	Internetrouter	139
5.2.2	Portfreigabe	140
5.2.3	IP-Forwarding	140
5.2.4	Firewall auf dem Tunnel	141
5.3	Testverbindung	142
5.4	Verbindungsarten	145
5.5	Die Konfigurationsdatei	147
5.6	Verbindungen mit statischem Schlüssel	149
5.6.1	Gateway-to-Gateway-Verbindung (G2G)	149
5.6.2	Client-to-Gateway-Verbindung (C2G)	154
5.6.3	Debug-Level	159
5.7	Zertifikatbasiert	163
5.7.1	Client-to-Gateway-Verbindung	163

5.7.2	Client-to-Network-Verbindung (C2N)	168
5.7.3	Network-to-Network-Verbindung (N2N)	175
5.7.4	Ethernet-Tunnel	179
5.8	Server-Login	184
5.8.1	Eigene Benutzerverwaltung unter Linux	185
5.8.2	Eigene Benutzerverwaltung unter Windows	187

6 Plugins 189

6.1	auth-pam-Plugin	190
6.2	Quellcode	190
6.3	Einsatz	190

7 Weitere Konfigurationen 193

7.1	Management-Interface	193
7.1.1	Management-Interface konfigurieren	194
7.1.2	Interface-Befehle	195
7.2	WLAN absichern	199
7.2.1	Szenario	200
7.2.2	Konfiguration	201
7.2.3	Verbindungsaufbau	203
7.2.4	Wichtige Optionen	204
7.3	Sichere Remotesteuerung	205
7.3.1	Firewall-Einstellungen	205
7.3.2	Konfiguration	207
7.3.3	Remotezugriff	208
7.4	OpenVPN auf einem PocketPC oder Smartphone	209
7.4.1	Installation	210
7.4.2	Konfiguration	213
7.4.3	Einschränkungen	216

8 Tipps 219

8.1	Sicherheiten	220
8.1.1	Server-Zertifikate	220
8.1.2	Zertifikate mit gleichem »Common Name«	221
8.1.3	OpenVPN-Benutzer	222
8.1.4	Verschlüsselung deaktivieren	224
8.2	Optimierungen	224
8.2.1	OpenVPN als Dämon	224

8.2.2	comp-lzo	229
8.2.3	Limitierte Bandbreite	230
8.2.4	Mehrere Server	230
8.3	Sonstige	231
8.3.1	Normaler Benutzer	231
8.3.2	push-Optionen	232
8.3.3	VPN-Gateway und Standardgateways	233
8.3.4	DNS unter Linux	233
8.3.5	IP-Forward per Skript	235

9 Fehlersuche und Probleme 237

9.1	OpenVPN startet nicht	238
9.1.1	Syntax- bzw. Parameterfehler	238
9.1.2	TUN-/TAP-Device wurde nicht gefunden	238
9.2	OpenVPN startet	239
9.2.1	Systemzeit	240
9.2.2	Zugriffsprobleme	240
9.2.3	Ein Ping kommt an, eine Datenübertragung ist jedoch nicht möglich	241
9.2.4	Die Verbindung bricht ständig ab	242
9.2.5	Unter Windows XP wird keine IP-Adresse zugewiesen	242
9.3	Fehler- und Warnmeldungen	242
9.3.1	Fehlermeldungen	243
9.3.2	Warnmeldungen	244

10 Optionen 247

10.1	Allgemeine Optionen	248
10.2	Tunnel	249
10.3	Server	268
10.4	Client	272
10.5	Data Channel Encryption	273
10.6	TLS-Mode	274
10.7	SSL-Informationen	277
10.8	Statischer Schlüssel	278
10.9	Windows-spezifische Optionen	278
10.10	Signale	282

11 Skripte 283

11.1 Zertifizierungsstelle erstellen 283

11.2 Zertifikate erstellen 285

11.3 Zertifikate sperren 286

Index 289