

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>15</b>
Aufbau	16
Danksagung	17
<b>1 Virtuelle private Netzwerke</b>	<b>19</b>
1.1 Was ist ein VPN?	19
1.2 Geschichte und Technologien	20
1.3 Warum VPNs?	24
1.4 Rahmenbedingungen für den Einsatz	26
1.5 Der VPN-Markt	28
1.6 IP-VPNs und das Internet	30
1.7 Entwicklungen und Ausblicke	33
<b>2 VPN-Typen</b>	<b>37</b>
2.1 Remote-Access-VPN	37
2.2 Branch-Office-VPN	41
2.3 Extranet-VPN	42
2.4 VPN-Service-Provider	43
2.4.1 IP-VPN-Dienste	44
2.4.2 Layer-2-VPN-Dienste	46
2.5 Intranet-VPN	47
2.5.1 Virtual Local Area Network (VLAN)	48
2.5.2 VLANs nach IEEE802.1q	50
2.5.3 IP-Tunneling	52
<b>3 Anforderungen an VPNs</b>	<b>53</b>
3.1 Sicherheit	53
3.1.1 Datenvertraulichkeit	53
3.1.2 Schlüsselmanagement	54
3.1.3 Paket-Authentifizierung	55
3.1.4 Datenintegrität	55
3.1.5 Benutzer-Authentifizierung	56
3.1.6 Benutzer-Autorisierung	56
3.1.7 Schutz vor Sabotage	57
3.1.8 Schutz vor unerlaubtem Eindringen	57

3.2	Verfügbarkeit	59
3.2.1	Die Verfügbarkeit von Wählverbindungen	59
3.2.2	Die Verfügbarkeit von permanenten Verbindungen	60
3.2.3	Die Verfügbarkeit von IP-VPNs	60
3.3	Performance	61
3.3.1	Die Performance von Wählverbindungen	61
3.3.2	Die Performance von permanenten Verbindungen	61
3.3.3	Die Performance von IP-VPNs	62
3.4	Quality-of-Service (QoS)	62
3.4.1	Einführung in QoS-Konzepte	63
3.4.2	Quality-of-Service bei Wählverbindungen	66
3.4.3	Quality-of-Service bei permanenten Verbindungen	67
3.4.4	Quality-of-Service im IP-Protokoll	69
3.4.5	Die IP-Differentiated-Services-Architektur (DiffServ)	69
3.4.6	Differentiated Services in IP-VPNs	74
3.5	Skalierbarkeit und Migrationsfähigkeit	75
3.6	Integration in existierende Netze	76
3.6.1	Management	76
3.6.2	Sicherheit	80
3.7	Koexistenz zu traditionellen WAN-Strukturen	82
3.8	Adressmanagement	83
3.9	Interoperabilität	85
<b>4</b>	<b>Sicherheitstechnologie</b>	<b>87</b>
4.1	Sicherheit in VPNs	87
4.1.1	Sicherheit in Unternehmensdatennetzen	87
4.1.2	Die Sicherheit von virtuellen privaten Netzen	90
4.1.3	Datenvertraulichkeit	91
4.1.4	Sicherheit in der Netzwerkschicht mit IP Security	93
4.1.5	Benutzer-Authentifizierung	95
4.2	Die Grundlagen der Kryptographie	95
4.2.1	Geschichtliches	95
4.2.2	Datenvertraulichkeit	97
4.2.3	Verschleierung und Verschlüsselung	97
4.2.4	Die Kunst der Kryptoanalyse	99

4.2.5	Einführung in die Kryptographie	101
4.2.6	Verschlüsselungsverfahren	108
4.3	Symmetrische Verschlüsselungsverfahren	113
4.4	Der Data Encryption Standard (DES)	114
4.4.1	Ein Überblick über DES	116
4.4.2	Die DES-Schlüsseltransformation	117
4.4.3	Die DES-Funktion	118
4.4.4	Die DES-Entschlüsselung	120
4.5	Triple-DES	120
4.6	Cipher Block Chaining (CBC)	122
4.6.1	Die Funktionsweise von CBC	123
4.7	Ausblick: Der Advanced Encryption Standard	124
4.7.1	AES-Software-Implementierung	126
4.7.2	AES-Hardware-Implementierung	126
4.7.3	AES-Geschwindigkeit und Optimierungsmöglichkeiten	127
4.7.4	»And the winner is .... Rijndael«	128
4.8	Asymmetrische Verschlüsselungsverfahren	129
4.8.1	Die kurze Geschichte der Public-Key-Kryptographie	129
4.8.2	Das Grundprinzip der Public-Key-Kryptographie	131
4.8.3	Mathematische Grundlagen	132
4.9	Das Diffie-Hellman-Verfahren	136
4.10	Das RSA-Verfahren	138
4.10.1	Zufallszahlen	140
4.11	Hashfunktionen	141
4.11.1	Algorithmen	142
4.11.2	Keyed Hashing	143
4.11.3	Hash-based Message Authentication Code (HMAC)	143
<b>5</b>	<b>Authentifizierung</b>	<b>145</b>
5.1	Möglichkeiten der Authentifizierung	146
5.1.1	Starke und schwache Authentifizierung	146
5.1.2	Wissensbasierende Authentifizierung	146
5.1.3	Besitzbasierende Authentifizierung	147
5.1.4	Kombinationsverfahren	147
5.1.5	Biometrik	148
5.1.6	Verfahren mit Einmal-Token	148

5.2	Digitale Signaturen und digitale Zertifikate	150
5.2.1	Funktionsweise von digitalen Signaturen	150
5.2.2	Digitale Zertifikate nach ITU-X.509-Standard	153
5.3	Authentifizierungssysteme und -protokolle	155
5.3.1	PAP und CHAP	155
5.3.2	RADIUS	157
5.3.3	LDAP	160
5.3.4	Chipkarten	160
5.4	Public Key Infrastructure (PKI)	162
5.4.1	Vertrauensmodelle	162
5.4.2	Die Certificate Authority (CA)	164
5.4.3	Die Registration Authority (RA)	164
5.4.4	Zertifikat-Management	164
5.4.5	Die Qual der Wahl: Öffentliche oder private Zertifikate	166
5.4.6	Das Signaturgesetz und die EU-Richtlinie	167
<b>6</b>	<b>Tunneling-Technologien im Überblick</b>	<b>169</b>
6.1	Tunneling-Modelle	170
6.1.1	Das Intra-Provider-Modell	170
6.1.2	Das Provider-Enterprise-Modell	171
6.1.3	Das Ende-zu-Ende-Modell	172
6.2	Tunneling-Protokolle	172
6.2.1	Layer-2-Tunneling-Protokolle	172
6.2.2	Layer-3-Tunneling-Protokolle	173
6.2.3	Multi Protocol Label Switching (MPLS)	174
6.3	Standardisierte Tunneling-Protokolle	176
6.3.1	IP Security Protocol (IPSec) im Tunnel-Modus	176
6.3.2	Layer 2 Tunneling Protocol (L2TP)	178
6.4	Nicht standardisierte Protokolle	179
6.4.1	Layer 2 Forwarding (L2F)	180
6.4.2	Point-to-Point Tunneling Protocol (PPTP)	180
6.5	Verschachtelte Tunneling-Protokolle	181
6.6	Welches Protokoll für welchen Zweck?	183
6.6.1	Gegenüberstellung	183
6.6.2	Auswahlkriterien	184

<b>7</b>	<b>Das IP-Security-Protokoll (IPSec)</b>	<b>187</b>
7.1	IP Security im Überblick	188
7.1.1	Paketintegrität	188
7.1.2	Paketauthentifizierung	189
7.1.3	Paketvertraulichkeit	189
7.1.4	Verkehrsflussvertraulichkeit	189
7.1.5	Schutz vor wiederholtem Senden von Paketen (Replay-Angriff)	190
7.1.6	Schutz vor weiteren Denial-of-Service-Angriffen	190
7.2	Kryptographische Verfahren in IPSec	191
7.2.1	Datenverschlüsselung in IPSec	191
7.2.2	Integritätsprüfung und Authentifizierung in IPSec	193
7.2.3	Schutz vor Replay-Angriffen	194
7.3	Die IPSec-Standardisierung	196
7.3.1	Die IPSec-Architektur	196
7.3.2	Die aktuelle IPSec-Standardisierung	197
7.4	Die IPSec-Sicherheitsassoziation	199
7.5	Die IPSec-Security-Policy	201
7.5.1	Die Security Policy in IPSec	201
7.5.2	Die IPSec-Selektoren	202
7.6	IPSec-Betriebsmodi	203
7.6.1	Tunnelmodus	203
7.6.2	Transportmodus	203
7.7	IPSec-Einsatzszenarien	204
7.7.1	Gateway-zu-Gateway	205
7.7.2	Host-zu-Gateway	205
7.7.3	Host-zu-Host	205
7.8	IPSec-Protokolle	205
7.8.1	Die Paketverarbeitung in IPSec	205
7.8.2	Das Authentication-Header-Protokoll (AH)	206
7.8.3	Das Encapsulating-Security-Payload-Protokoll (ESP)	209
7.9	IPSec-Implementierungen	214
7.9.1	Betriebssystemebene, IPSec-Stack	214
7.9.2	Bump-in-the-Stack (BITS)	215
7.10	Betrachtungen zur IPSec-Performance	215
7.11	Zukünftige Entwicklungen	219

<b>8</b>	<b>Das Internet-Key-Exchange-Protokoll</b>	<b>221</b>
8.1	Das Henne-Ei-Problem	221
8.2	ISAKMP	222
8.2.1	Die Sicherheit von ISAKMP	223
8.2.2	Der ISAKMP-Header	228
8.2.3	Der generische ISAKMP-Nutzdaten-Header	231
8.3	ISAKMP-Nutzdaten	232
8.3.1	Die Sicherheitsassoziation-Payload	232
8.3.2	Die Proposal Payload	233
8.3.3	Die Transform Payload	233
8.3.4	Key Exchange Payload	234
8.3.5	Identification Payload	235
8.3.6	Certificate Payload	235
8.3.7	Certificate Request Payload	236
8.3.8	Hash, Signature und Nonce Payload	237
8.3.9	Notification Payload	238
8.3.10	Delete Payload	239
8.3.11	Vendor ID Payload	240
8.3.12	Die ISAKMP-Phasen	241
8.3.13	Die ISAKMP-Austauschvorgänge	241
8.4	Das Oakley Key Determination Protocol	243
8.4.1	Die Oakley-Gruppe-1	243
8.4.2	Die Oakley-Gruppen 2 bis 5	244
8.5	Der Aufbau von IKE	244
8.5.1	Perfect Forwarding Secrecy	245
8.5.2	Die Attribute einer IPsec-Sicherheitsassoziation	245
8.5.3	Die Attribute einer ISAKMP-Sicherheitsassoziation	247
8.5.4	IKE-Sicherheitsverfahren	250
8.5.5	Die Schlüsselerzeugung in IKE	251
8.5.6	IKE-Authentifizierung	254
8.6	Der IKE Main Mode	256
8.6.1	Authentifizierung mit Pre-Shared Key	256
8.6.2	Authentifizierung mit digitaler Signatur	260
8.6.3	Authentifizierung mit Public-Key-Verschlüsselung (RSA)	261

8.6.4	Authentifizierung mit revidierter Public-Key-Verschlüsselung (RSA)	263
8.7	Der IKE Aggressive Mode	265
8.7.1	Authentifizierung mit Pre-Shared-Secret	267
8.7.2	Authentifizierung mit digitaler Signatur	269
8.7.3	Authentifizierung mit standardisierter und revidierter Public-Key-Verschlüsselung	269
8.8	Der IKE Quick Mode	269
8.9	Die Performance von IKE	272
8.9.1	IKE und Hardwarebeschleuniger	273
<b>9</b>	<b>Das Layer 2 Tunneling Protocol</b>	<b>277</b>
9.1	Das Point-to-Point Protocol (PPP)	277
9.1.1	PPP-Remote-Access	278
9.1.2	PPP-Komponenten	278
9.1.3	PPP-Steuerungsprotokolle und -Dienste	280
9.1.4	PPP-Verbindungsaufbau	282
9.2	PPP-Tunneling mit L2TP	284
9.2.1	Virtueller Remote Access mit L2TP	285
9.2.2	PPP-Session-Verteilung in L2TP	286
9.2.3	Die Rolle des LAC (L2TP Access Concentrator)	289
9.2.4	Die Rolle des LNS (L2TP Network Server)	289
9.2.5	Betrachtungen zur Performance von L2TP	289
9.2.6	L2TP-Tunneling-Modelle	292
9.2.7	L2TP-Paketformate	293
9.2.8	L2TP Attribute Value Pairs (AVP)	295
9.2.9	Auf- und Abbau von Tunneln und Calls in L2TP	298
9.2.10	L2TP-Benutzer-Authentifizierung	300
9.3	Die Sicherheit von L2TP	303
9.4	IPSec secured L2TP	305
<b>10</b>	<b>VPN-Design</b>	<b>309</b>
10.1	Ein VPN ist auch nur ein Netzwerk	309
10.2	Die Planung	310
10.3	Die Ist-Aufnahme	310
10.3.1	Technische Aspekte	312
10.3.2	Betriebswirtschaftliche Aspekte	314
10.3.3	Sicherheit	315

10.4	Der Sollzustand	316
10.4.1	Der unvermeidliche (?) Bruch	316
10.4.2	Randbedingungen	317
10.4.3	Technische Aspekte	319
10.4.4	Betriebswirtschaftliche Aspekte	321
10.5	Die Übergangsphase	322
10.6	Die Sicherheitsstrategie	322
10.7	Auswahl der VPN-Technologie	325
10.7.1	VPN-Typ	325
10.7.2	Tunneling-Protokolle	326
10.8	Ermitteln der QoS-Parameter	327
10.9	Die Realisierung	328
10.9.1	Routing im VPN	329
10.9.2	Remote Access	330
10.9.3	Kleine Außenstellen und Heimbüros	341
10.9.4	Skalierbarkeit	342
10.9.5	Redundanz und Ausfallsicherheit	343
10.9.6	Durchsatz und Quality-of-Service	344
10.9.7	Sicherheitsstrategie und Firewalls	346
10.9.8	Authentifizierungsverfahren	351
10.9.9	Die Auswahl von Service Providern	352
10.9.10	Service Level Agreements	353
10.10	Beispiele	356
10.10.1	Remote-Access-VPN	356
10.10.2	Branch-Office-VPN	359
10.10.3	IP-VPN-Service eines ISP	360
<b>11</b>	<b>Auswahl der VPN-Komponenten</b>	<b>361</b>
11.1	VPN, Feature oder dediziert?	362
11.2	Performance	363
11.2.1	Eigene Messungen	364
11.2.2	Veröffentlichte Testberichte	364
11.2.3	Beurteilungskriterien	364
11.3	Die Herstellerauswahl	366
11.4	Die Auswahl der VPN-Komponenten	370
11.4.1	Das Beispielnetzwerk	370
11.4.2	Allgemein	372

11.4.3	Leistung	373
11.4.4	Schnittstellen	375
11.4.5	Tunneling-Protokolle	376
11.4.6	Sicherheit	377
11.4.7	Authentifizierung	379
11.4.8	Quality-of-Service und Profile	380
11.4.9	Management, Accounting, Logging und weitere Funktionen	382
11.4.10	VPN-Routing	384
11.5	Die Auswahl von VPN-Clientsoftware	385
<b>12</b>		
	<b>Fallstudien</b>	<b>389</b>
12.1	Studie 1: Die Software AG	389
12.1.1	Zum Unternehmen	389
12.1.2	Das Projekt	390
12.1.3	Projektablauf und Realisierung	391
12.2	Studie 2: Der Blutspendedienst des DRK	392
12.2.1	Zu den Unternehmen	393
12.2.2	Das Projekt	394
12.2.3	Projektablauf und Realisierung	395
12.3	VPN-Dienste von Service Providern	398
12.4	Studie 3: Die VIAG Interkom	399
12.4.1	Zum Unternehmen	399
12.4.2	Der IP-VPN-Dienst	400
12.4.3	Infrastruktur	404
12.4.4	Remote-Access-VPN	405
12.4.5	Branch-to-Branch-VPN	406
<b>13</b>	<b>Anhang</b>	<b>409</b>
	Weiterführende Literatur	409
	Links	411
<b>14</b>	<b>Stichwortverzeichnis</b>	<b>413</b>