

Inhaltsübersicht

Vorwort zur 2. Auflage	29
Einleitung	31
Teil I Firewall-Grundlagen	33
1 Firewall-Geschichte	35
2 Firewall-Technologien	39
3 Firewall-Architekturen	43
4 Bedrohungen bei der Vernetzung von Systemen	49
Teil II Firewalls mit Iptables – Einführung	73
5 Eine einfache Firewall mit Iptables	75
6 Härtung eines Linux-Systems	131
Teil III Typische Firewall-Konfigurationen	149
7 Eine lokale Firewall	151
8 Aufbau einer DMZ	163
Teil IV Werkzeuge	189
9 Zentrale Protokollserver	191
10 Zentrale Zeitsynchronisation	211
11 Protokollanalyse	221

12 Administrationsoberflächen 239

13 Distributionswerkzeuge 261

14 Firewall-Distributionen 273

15 Testmethoden und -werkzeuge 285

Teil V Fortgeschrittene Konfiguration 319

16 Die Iptables-Standardtests 321

17 Alle Ziele 345

18 Patch-O-Matic 355

19 Connection Tracking 357

20 Die nat-Tabelle 367

21 Die Mangle-Tabelle 377

22 Die Raw-Tabelle 381

23 Das /proc-Dateisystem 383

24 Fortgeschrittene Protokollierung 413

25 Conntrack-Tools 423

26 Ipset 427

27 Hochverfügbare Firewalls 439

28 Transparente Proxies 459

Teil VI	Transparente Firewalls	463
29	ProxyARP	465
30	Iptables auf einer Bridge	469
31	ebtables	475
Teil VII	Protokolle und Applikationen	487
32	Behandlung einzelner Protokolle	489
33	L7-Filter	525
34	IPsec	531
35	ICMP	543
Teil VIII	IPv6	559
36	Das IPv6-Protokoll	561
37	Transitionsmechanismen	579
38	Kleines IPv6-Howto	583
39	Filterung mit ip6tables	595
40	Neue IPv6-Targets	597
41	Neue IPv6-Matches	599
42	Empfohlene IPv6-Regeln	603
A	Netzwerkgrundlagen	611
	Literaturverzeichnis	639
	Stichwortverzeichnis	641

Inhaltsverzeichnis

Vorwort zur 2. Auflage	29
Einleitung	31
I Firewall-Grundlagen	33
1 Firewall-Geschichte	35
1.1 Der Anfang des Internets	35
1.2 Der Morris-Wurm	36
1.3 Die erste Firewall	36
1.4 Firewalls heute	37
2 Firewall-Technologien	39
2.1 Paketfilter	39
2.2 Zustandsorientierte Paketfilter	40
2.3 Circuit Relay	40
2.4 Application-Level-Gateway (Proxy)	41
2.5 Network-Address-Translation	41
3 Firewall-Architekturen	43
3.1 Screening-Router	43
3.2 DMZ	44
3.3 Multiple DMZ	46
3.4 Wahl der Architektur	47
4 Bedrohungen bei der Vernetzung von Systemen	49
4.1 Angreifer und Motivation	49
4.1.1 Der klassische Hacker	49
4.1.2 Skript-Kiddies	50
4.1.3 Insider	50
4.1.4 Mitbewerber	50
4.1.5 Geheimdienste	51
4.1.6 Terroristen und organisierte Kriminalität	51
4.2 Tendenzen und Entwicklungen	52
4.3 Schutzziele	53

4.4	Angriffsmethoden	54
4.4.1	Denial-of-Service (DoS)	55
4.4.2	Spoofing	56
4.4.3	Session Hijacking	61
4.4.4	Bufferoverflow	62
4.4.5	Formatstring-Angriffe	66
4.4.6	Race-Condition	67
4.4.7	SQL-Injektion	70
4.4.8	Welchen Schutz bietet eine Firewall?	72
 II Firewalls mit Iptables – Einführung		73
5	Eine einfache Firewall mit Iptables	75
5.1	Netfilter und Iptables	75
5.2	Der Iptables-Befehl und die Filter-Tabelle	75
5.3	Ihr erstes Firewall-Skript	82
5.3.1	Fehlersuche	90
5.4	Einbindung in den Bootprozess	91
5.5	Connection Tracking und Netzwerkverbindungen	94
5.5.1	Der zustandslose Paketfilter IPchains	94
5.5.2	IPchains und UDP	95
5.5.3	IPchains und TCP	97
5.5.4	IPchains und ICMP	100
5.5.5	IPchains und Masquerading	101
5.5.6	Iptables und Conntrack	101
5.5.7	Conntrack und UDP	103
5.5.8	Conntrack und TCP	105
5.5.9	Conntrack und ICMP	107
5.5.10	Conntrack und alle weiteren generischen Protokolle	109
5.6	Filterregeln	109
5.7	Die NAT-Tabelle und -Regeln	111
5.7.1	Source-NAT	113
5.7.2	Destination-NAT	115
5.8	NAT-Beispiel	116
5.9	Die Mangle-Tabelle	120
5.10	Die Raw-Tabelle	122

- 5.11 Einstellungen des Kernels 122
 - 5.12 Protokollierung 125
 - 5.13 Test der Firewall 128
- 6 Härtung eines Linux-Systems 131**
 - 6.1 Warum sollte eine Firewall gehärtet werden? 131
 - 6.2 Installation des Linux-Systems 132
 - 6.3 Updates 134
 - 6.3.1 Debian/Ubuntu-Updates 135
 - 6.3.2 OpenSUSE-Updates 135
 - 6.3.3 Fedora-Updates 136
 - 6.4 Deaktivieren überflüssiger Dienste 136
 - 6.4.1 Startskripte 136
 - 6.5 Internet-Super-Server 137
 - 6.5.1 Der Cron-Daemon 137
 - 6.6 Entfernen überflüssiger Software 138
 - 6.7 Sicherheit auf Dateisystemebene 139
 - 6.8 Sicherheit beim Bootvorgang 141
 - 6.9 Bastille-Linux 142
 - 6.10 SELinux und AppArmor 142
 - 6.11 POSIX-ACLs 143
 - 6.12 Intrusion-Detection- und -Prevention-Systeme 145
 - 6.12.1 Intrusion-Detection-Systeme 145
 - 6.12.2 Intrusion-Prevention-Systeme 146
- III Typische Firewall-Konfigurationen 149**
- 7 Eine lokale Firewall 151**
 - 7.1 Wieso eine lokale Firewall? 151
 - 7.2 Die Ketten 152
 - 7.3 Die Owner-Erweiterung 157
 - 7.4 Kombination mit Gateway-Regeln 160
- 8 Aufbau einer DMZ 163**
 - 8.1 DMZ-Architekturen 163
 - 8.2 Dreibeiniger Paketfilter mit DMZ 163
 - 8.3 Optimierung mit benutzerdefinierten Ketten 172
 - 8.3.1 Anwendung der benutzerdefinierten Ketten 176

8.4	DMZ mit zwei Paketfiltern	181
8.4.1	Der äußere Paketfilter	182
8.5	Der innere Paketfilter	186
IV	Werkzeuge	189
9	Zentrale Protokollserver	191
9.1	Einrichtung eines zentralen Protokollservers	191
9.2	Rsyslogd	195
9.2.1	Rsyslogd-Funktionen	195
9.2.2	Rsyslogd-Anwendung	196
9.3	Syslog-ng	197
10	Zentrale Zeitsynchronisation	211
10.1	Das Zeitsynchronisationsprotokoll NTP	211
10.2	Der ntpd-Zeitserver	212
10.2.1	Der Client	212
10.2.2	Der Server	215
10.3	Sicherheit	215
10.3.1	Symmetrische Authentifizierung	216
10.3.2	Asymmetrische Authentifizierung	217
11	Protokollanalyse	221
11.1	Fwlogwatch	221
11.1.1	Installation von Fwlogwatch	221
11.2	Konfiguration von Fwlogwatch	222
11.3	IP Tables State (IPTState)	231
11.4	Webfwlog Firewall Log Analyzer	234
11.5	NuLog2	236
11.6	EpyLog Log Analyzer	237
12	Administrationsoberflächen	239
12.1	Firewall Builder	239
12.2	Firestarter	248
12.3	Shorewall (Shoreline Firewall)	253
12.3.1	Das Shorewall-Konzept	253
12.3.2	Die Shorewall-Dateien	256
12.3.3	Weitere Shorewall-Eigenschaften	260

- 13 Distributionswerkzeuge 261**
 - 13.1 Fedora 261
 - 13.2 OpenSUSE 261
 - 13.3 Debian 271
- 14 Firewall-Distributionen 273**
 - 14.1 IPCop 273
 - 14.1.1 Das IPCop-Konzept 273
 - 14.1.2 IPCop-Installation 274
 - 14.1.3 IPCop-Web-Interface 278
- 15 Testmethoden und -werkzeuge 285**
 - 15.1 Test der Regeln 285
 - 15.2 Fehlersuche am Beispiel 287
 - 15.3 Nmap 290
 - 15.3.1 Nmap-Installation 290
 - 15.3.2 Einfache Scans 292
 - 15.3.3 Fortgeschrittene Anwendung 298
 - 15.4 Decoy-Scan 302
 - 15.5 Banner-Grabbing 303
 - 15.6 Idle-Scan 304
 - 15.6.1 Modifikation des Client-Ports, Time-Tuning und Fragmentierung . 305
 - 15.6.2 Ausgabeformate 307
 - 15.6.3 Nmap-Hilfswerkzeuge 308
 - 15.7 Nessus und OpenVAS 310

V Fortgeschrittene Konfiguration 319

- 16 Die Iptables-Standardtests 321**
 - 16.1 Eingebaute Funktionen 321
 - 16.1.1 -p, --protocol 321
 - 16.1.2 -s, --source 321
 - 16.1.3 -d, --destination 321
 - 16.1.4 -i, --in-interface 322
 - 16.1.5 -o, --out-interface 322
 - 16.1.6 -f, --fragment 322

16.2	TCP-Tests	322
16.2.1	--sourceport	322
16.2.2	--destinationport	323
16.2.3	--tcp-flags	323
16.2.4	--syn	323
16.2.5	--tcp-option	323
16.3	UDP-Tests	323
16.3.1	--sourceport	324
16.3.2	--destinationport	324
16.4	ICMP-Tests	324
16.5	Weitere Erweiterungen	325
16.5.1	addrtype	325
16.5.2	ah	325
16.6	cluster	326
16.7	comment	327
16.8	connbytes	328
16.8.1	connlimit	328
16.8.2	connmark	329
16.8.3	conntrack	329
16.9	dccp	329
16.9.1	dscp	329
16.9.2	ecn	330
16.9.3	esp	330
16.9.4	hashlimit	330
16.9.5	helper	332
16.9.6	iprange	333
16.9.7	length	333
16.9.8	limit	333
16.9.9	mac	334
16.9.10	mark	334
16.9.11	multiport	334
16.10	osf	334
16.10.1	owner	335
16.10.2	physdev	335
16.10.3	pkttype	336
16.10.4	policy	336

- 16.10.5 quota 336
- 16.10.6 rateest 336
- 16.10.7 realm 337
- 16.10.8 recent 338
- 16.10.9 sctp 339
- 16.10.10 set 339
- 16.10.11 socket 340
- 16.10.12 state 340
- 16.10.13 statistic 340
- 16.10.14 string 340
- 16.10.15 tcpmss 341
- 16.10.16 time 341
- 16.10.17 tos 341
- 16.10.18 ttl 342
- 16.10.19 u32 342
- 17 Alle Ziele 345**
 - 17.1 ACCEPT 345
 - 17.2 CLASSIFY 345
 - 17.3 CLUSTERIP 345
 - 17.4 CONNMARK 347
 - 17.5 CONNSECMARK 347
 - 17.6 DNAT 347
 - 17.7 DROP 347
 - 17.8 DSCP 347
 - 17.9 ECN 347
 - 17.10 LOG 347
 - 17.11 MARK 348
 - 17.12 MASQUERADE 348
 - 17.13 NETMAP 348
 - 17.14 NFLOG 348
 - 17.15 NFQUEUE 349
 - 17.16 NOTRACK 349
 - 17.17 RATEEST 349
 - 17.18 REDIRECT 349
 - 17.19 REJECT 349

17.20	RETURN	350
17.21	SAME	350
17.22	SECMARK	350
17.23	SET	350
17.24	SNAT	350
17.25	TCPMSS	350
17.26	TCPOPTSTRIP	352
17.27	TEE	352
17.28	TOS	352
17.29	TPROXY	353
17.30	TRACE	353
17.31	TTL	353
17.32	ULOG	353
18	Patch-O-Matic	355
19	Connection Tracking	357
19.1	Connection Tracking – Überblick	357
19.1.1	Das TCP-Connection-Tracking	358
19.1.2	Das UDP-Connection-Tracking	359
19.1.3	Das ICMP-Connection-Tracking	359
19.1.4	Das Connection Tracking für alle weiteren Protokolle	360
19.2	Das nf_conntrack-Kernelmodul	360
19.3	/proc-Variablen	362
19.3.1	nf_conntrack_acct	362
19.3.2	nf_conntrack_buckets	362
19.3.3	nf_conntrack_checksum	362
19.3.4	nf_conntrack_count	362
19.3.5	nf_conntrack_generic_timeout	363
19.3.6	nf_conntrack_icmp_timeout	363
19.3.7	nf_conntrack_icmpv6_timeout	363
19.3.8	nf_conntrack_log_invalid	363
19.3.9	nf_conntrack_max	363
19.3.10	nf_conntrack_tcp_be_liberal	363
19.3.11	nf_conntrack_tcp_loose	363
19.3.12	nf_conntrack_tcp_max_retrans	364
19.3.13	nf_conntrack_tcp_timeout_close	364

- 19.3.14 nf_conntrack_tcp_timeout_close_wait 364
 - 19.3.15 nf_conntrack_tcp_timeout_established 364
 - 19.3.16 nf_conntrack_tcp_timeout_fin_wait 364
 - 19.3.17 nf_conntrack_tcp_timeout_last_ack 364
 - 19.3.18 nf_conntrack_tcp_timeout_max_retrans 365
 - 19.3.19 nf_conntrack_tcp_timeout_syn_recv 365
 - 19.3.20 nf_conntrack_tcp_timeout_syn_sent 365
 - 19.3.21 nf_conntrack_tcp_timeout_time_wait 365
 - 19.3.22 nf_conntrack_udp_timeout 365
 - 19.3.23 nf_conntrack_udp_timeout_stream 365
- 19.4 TCP-Zustände 366
- 20 Die nat-Tabelle 367**
 - 20.1 Die NAT-Tabelle und ihre Ketten 367
 - 20.2 Source-NAT 369
 - 20.3 Destination-NAT 370
 - 20.4 MASQUERADE 370
 - 20.5 NETMAP 371
 - 20.6 SNAT 372
 - 20.7 SAME 373
 - 20.8 DNAT 373
 - 20.9 REDIRECT 374
 - 20.10 NAT-Helfermodule 374
 - 20.11 Das CONNMARK-Target 375
- 21 Die Mangle-Tabelle 377**
 - 21.1 Die Ketten der mangle-Tabelle 377
 - 21.2 Aktionen der Mangle-Tabelle 377
 - 21.3 CLASSIFY 377
 - 21.4 CONNMARK 378
 - 21.5 DSCP 378
 - 21.6 ECN 378
 - 21.7 MARK 379
 - 21.8 TOS 379
 - 21.9 TPROXY 379
 - 21.10 TTL 380

22 Die Raw-Tabelle	381
22.1 Die Raw-Tabelle	381
23 Das /proc-Dateisystem	383
23.1 Einführung in /proc	383
23.2 /proc/net/	385
23.2.1 ip_conntrack oder nf_conntrack	386
23.2.2 nf_conntrack_expect	386
23.2.3 ip_tables_*	386
23.3 /proc/sys/net/ipv4	386
23.3.1 icmp_*	386
23.3.2 igmp_*	388
23.3.3 inet_peer_*	389
23.3.4 ip_*	389
23.3.5 ipfrag_*	391
23.3.6 tcp_*	391
23.3.7 udp_*	401
23.3.8 cipso_*	402
23.3.9 /proc/sys/net/ipv4/conf	402
23.3.10 /proc/sys/net/netfilter	407
23.3.11 /proc/sys/net/ipv6	407
23.3.12 /proc/sys/net/ipv6/conf/	407
23.3.13 /proc/sys/net/bridge/proc/sys/net/	411
24 Fortgeschrittene Protokollierung	413
24.1 Das ULOG-Target	413
24.2 Das ipt_ULOG-Kernelmodul	414
24.3 Der Ulogd-Daemon	414
24.3.1 [OPRINT]	418
24.3.2 [LOGEMU]	419
24.3.3 [MYSQL]	419
24.3.4 [PGSQL]	419
24.3.5 [PCAP]	420
24.3.6 [SQLITE3]	420
24.3.7 [SYSLOG]	421
24.4 Der Specter-Daemon	421

25	Conntrack-Tools	423
26	Ipset	427
26.1	ipset Version 4 und iptables	427
26.1.1	Die Ipset-4-Typen	429
26.1.2	ipmap	429
26.1.3	Das Kommando ipset in der Version 4	432
26.2	ipset Version 6 und ip6tables	433
26.2.1	ipset Version 6: Syntax	434
26.2.2	Die Ipset-6-Typen	434
27	Hochverfügbare Firewalls	439
27.1	Was ist Hochverfügbarkeit, und wo ist das Problem?	439
27.2	Einfache Hochverfügbarkeit	440
27.3	Hochverfügbarkeit bei zustandsorientierten Firewalls	441
27.4	Automatische Erkennung aufgebauter Verbindungen nach dem Fail-Over	441
27.4.1	Praktische Implementierung mit KeepAlived	443
27.4.2	Hochverfügbarkeit und Masquerading/NAT	446
27.5	Zustandssynchronisation mit conntrackd	447
27.5.1	Synchronisationsprotokolle	447
27.5.2	Aufbau eines Active/Backup-Conntrackd-Clusters	449
28	Transparente Proxies	459
28.1	Client-transparenter Proxy	459
28.2	Voll-transparenter Proxy	460
VI	Transparente Firewalls	463
29	ProxyARP	465
29.1	Wie funktioniert ProxyARP?	465
29.2	ProxyARP-Konfiguration	466
29.3	Filterung mit Iptables	467
29.4	Fazit	468
30	Iptables auf einer Bridge	469
30.1	Wie funktioniert die Bridge?	469
30.2	Bau einer Bridge mit Linux	470
30.3	Filtern auf der Bridge mit iptables	472

30.4	Filtern auf der Bridge mit arptables	473
30.5	Fazit	474
31	ebtables	475
31.1	Ebtables-Installation	475
31.1.1	Konfiguration des Linux-Kernels	475
31.1.2	Installation des Userspace-Werkzeugs	476
31.2	Die Ebtables-Tabellen	476
31.2.1	Der Rahmen erreicht das System über ein Bridge-Interface	476
31.2.2	Der Rahmen erreicht das System über ein Nicht-Bridge-Interface	479
31.2.3	Ein lokal erzeugtes Paket verlässt das System über die Bridge . .	479
31.3	Die broute-Tabelle	479
31.4	Die ebtables-Syntax	480
31.5	Start einer Bridge auf Linux	485
31.5.1	Bridge auf Fedora	485
31.5.2	Bridge auf Debian	486

VII
Protokolle und Applikationen
487

32	Behandlung einzelner Protokolle	489
32.1	DHCP	489
32.1.1	Das DHCP-Protokoll	490
32.1.2	Iptables-Regeln	490
32.2	DNS	491
32.2.1	Das DNS-Protokoll	491
32.2.2	Iptables-Regeln	492
32.3	HTTP/HTTPS/Proxy	494
32.3.1	Iptables-Regeln	496
32.4	ELSTER	496
32.4.1	Iptables-Regeln	497
32.5	Telnet	498
32.5.1	Iptables-Regeln	498
32.6	SSH	499
32.6.1	Iptables-Regeln	499

- 32.7 P2P: Edonkey 500
 - 32.7.1 Iptables-Regeln 500
- 32.8 P2P: KaZaA 501
 - 32.8.1 Iptables-Regeln 502
- 32.9 P2P: BitTorrent 502
 - 32.9.1 Iptables-Regeln 503
- 32.10 FTP 504
 - 32.10.1 Das FTP-Protokoll 504
 - 32.10.2 Stateful Inspection des FTP-Protokolls 506
 - 32.10.3 Iptables-Regeln 507
- 32.11 SNMP 508
 - 32.11.1 Iptables-Regeln 509
- 32.12 Amanda 509
 - 32.12.1 Das Amanda-Protokoll 510
 - 32.12.2 Iptables-Regeln 510
- 32.13 PPTP 511
 - 32.13.1 Iptables-Regeln 511
- 32.14 SMTP 513
 - 32.14.1 Das SMTP-Protokoll 513
 - 32.14.2 Iptables-Regeln 514
- 32.15 IRC 515
 - 32.15.1 Iptables-Regeln 515
- 32.16 TFTP 516
 - 32.16.1 Iptables-Regeln 516
- 32.17 IMAP 517
- 32.18 Iptables-Regeln 518
- 32.19 POP3 518
 - 32.19.1 Iptables-Regeln 519
- 32.20 NTP 520
 - 32.20.1 Iptables-Regeln 520
- 32.21 NNTP 520
 - 32.21.1 Iptables-Regeln 520
- 32.22 H.323 521
 - 32.22.1 Iptables-Regeln 521

32.23	SIP	522
32.23.1	Iptables-Regeln	522
33	L7-Filter	525
33.1	L7-Hintergründe	526
33.2	L7: Kernel-Version	526
33.2.1	Nutzung der Kernel-Version	526
33.3	L7: Userspace-Version	527
33.3.1	Nutzung der Userspace-Version	527
33.4	Eigene L7-Protokolle	529
34	IPsec	531
34.1	IPsec-Grundlagen	531
34.2	Iptables-Regeln zum Durchleiten von IPsec	532
34.3	IPsec und Firewall auf demselben System	533
34.3.1	Transport-Modus	534
34.3.2	Tunnel-Modus	534
34.4	Filterung mit dem policy-Match	540
35	ICMP	543
35.1	ICMP-Grundlagen	543
35.2	destination-unreachable	544
35.3	fragmentation-needed	546
35.3.1	MTU und die Path-MTU-Discovery	546
35.4	source-quench	549
35.5	redirect	550
35.6	time-exceeded	550
35.7	parameter-problem	551
35.8	router-advertisement/router-solicitation	551
35.9	timestamp-request/timestamp-reply	552
35.10	address-mask-request/address-mask-reply	553
35.11	echo-request/echo-reply (Ping)	553
35.12	Traceroute	554
35.12.1	Optimierung der ICMP-Regeln	557

VIII IPv6	559
36 Das IPv6-Protokoll	561
36.1 Hintergründe und Geschichte	561
36.2 Überblick über die Änderungen und Neuerungen	563
36.3 IPv6-Adressen und ihre Notation	564
36.3.1 Adressen	564
36.3.2 Netzmaske	565
36.4 Adressarten und Scopes	566
36.4.1 Adressarten	567
36.4.2 Scope	569
36.5 IPv6-Multicast	570
36.6 Autokonfiguration	571
36.6.1 DHCP	574
36.7 Neighbor Discovery	575
36.8 Privacy Extensions	577
37 Transitionsmechanismen	579
37.1 NAT64	581
38 Kleines IPv6-Howto	583
38.1 Anbindung über einen Tunnelbroker	583
38.1.1 Freenet6	583
38.1.2 SixXS	586
38.2 Verteilung der IP-Adressen mit radvd	587
38.3 Nutzung von DHCPv6	588
38.3.1 Stateless DHCPv6	589
38.3.2 Stateful DHCPv6	590
38.4 NAT64 und DNS64	592
39 Filterung mit iptables	595
40 Neue IPv6-Targets	597
40.1 HL	597
41 Neue IPv6-Matches	599
41.1 dst	599
41.2 eui64	599
41.3 frag	599

41.4	hbh	600
41.5	hl	600
41.6	ipv6header	600
41.7	mh	600
41.8	rt	601
42	Empfohlene IPv6-Regeln	603
42.1	ICMPv6-Regeln	603
42.1.1	ICMPv6 – eine kurze Wiederholung	603
42.1.2	ICMPv6 aus Sicht der Firewall	604
42.1.3	ICMPv6-Filter für weiterzuleitenden Verkehr	605
42.1.4	ICMPv6-Filter für lokalen Verkehr	606
42.2	Weitere IPv6-spezifische Regeln	608
A	Netzwerkgrundlagen	611
A.1	TCP/IP	611
A.2	IPv4	611
A.2.1	Version	612
A.2.2	Header-Länge	612
A.2.3	Type of Service	613
A.2.4	Paketlänge	613
A.2.5	Identifikationsnummer	614
A.2.6	Flaggen	614
A.2.7	Fragment-Offset	614
A.2.8	Time To Live (TTL)	615
A.2.9	Protokoll	615
A.2.10	Prüfsumme	615
A.2.11	Quell-IP-Adresse	616
A.2.12	Ziel-IP-Adresse	616
A.2.13	IP-Optionen	616
A.3	UDP	618
A.4	TCP	619
A.4.1	Auf- und Abbau einer TCP-Verbindung	620
A.4.2	TCP-Header	622
A.5	Quell- und Zielport	623
A.6	Sequenznummer	623
A.7	Acknowledgement-Nummer	623

INHALTSVERZEICHNIS

- A.8 Header-Länge 624
- A.9 Reservierte Bits 624
- A.10 TCP-Flags 624
- A.11 Receive Window 625
- A.12 TCP-Prüfsumme 625
- A.13 Urgent-Zeiger 626
- A.14 TCP-Optionen 626
- A.15 Fortgeschrittene Eigenschaften von TCP 627
 - A.15.1 Flusskontrolle 627
 - A.15.2 Zuverlässigkeit 628
 - A.15.3 Explicit Congestion Notification 629
- A.16 ICMP 631
 - A.16.1 destination-unreachable 633
 - A.16.2 source-quench 633
 - A.16.3 time-exceeded 634
 - A.16.4 redirect 634
 - A.16.5 parameter-problem 634
 - A.16.6 echo-request und echo-reply 635
 - A.16.7 address-mask-request und address-mask-reply 635
 - A.16.8 timestamp-request und timestamp-reply 636
 - A.16.9 router-solicitation und router-advertisement 636
- A.17 ARP 636
- Literaturverzeichnis 639**
- Stichwortverzeichnis 641**