
Norbert Pohlmann

Firewall-Systeme

Sicherheit für Internet und Intranet

An International Thomson Publishing Company

Bonn • Albany • Belmont • Boston • Cincinnati • Detroit • Johannesburg • London
Madrid • Melbourne • Mexico City • New York • Paris • Singapore • Tokyo





Inhaltsverzeichnis

	Vorwort	17
1	Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit	23
2	Ziele von Firewall-Systemen	33
2.1	Analogien zu Firewall-Systemen	33
2.2	Zielsetzung eines Firewall-Systems	36
3	TCP/IP-Technologie für Internet und Intranet	41
3.1	Von den Anfängen bis heute	41
3.2	Vorteile der TCP/IP-Technologie	43
3.3	Das OSI-Referenzmodell	44
3.4	TCP/IP-Protokollarchitektur	47
3.5	Internet-Adressen	48
3.6	Die Kommunikationsprotokolle	51
3.6.1	IP-Protokoll	52
3.6.2	Routing Protokolle	54
3.6.3	ICMP	55
3.6.4	Portnummern	57
3.6.5	UDP	59
3.6.6	TCP	60
3.6.7	DNS	63
3.6.8	Telnet	63
3.6.9	FTP	64
3.6.10	SMTP	65
3.6.11	HTTP	66
3.6.12	NNTP	69
4	Bedrohungen aus dem Netz	71
4.1	Angriffsmöglichkeiten in Kommunikations-Systemen	71
4.1.1	Passive Angriffe	72

4.1.2	Aktive Angriffe	76
4.1.3	Zufällige Verfälschungsmöglichkeiten	79
4.2	Weitere Aspekte potentieller Bedrohungen bei der Kommunikation über das Internet	80
4.2.1	Angriffstools aus dem Internet	82
4.2.2	Implementierungsfehler in Anwendungen und fehlerhafte Konfiguration	82
4.3	Wie hoch ist das Risiko?	83
4.4	Schadenskategorien und Folgen	85
4.4.1	Verstoß gegen Gesetze/Vorschriften/Verträge	85
4.4.2	Beeinträchtigung der persönlichen Unversehrtheit	86
4.4.3	Beeinträchtigung der Aufgabenerfüllung	86
4.4.4	Negative Außenwirkung	86
4.4.5	Finanzielle Auswirkungen	87
4.5	Angriffsmethoden und prinzipielle Gegenmaßnahmen auf der Grundlage der TCP/IP-Protokolle	88
4.5.1	Idee eines Angriffes	88
4.5.2	Analyse des Netzes mit Hilfe von Scannerprogrammen	89
4.5.3	Paßword-Snooping und IP-Maskerade	91
4.5.4	Nutzung einer falschen Konfiguration	93
4.5.5	Hopping (Telnet)	95
4.5.6	Nutzung von Implementierungsfehlern in Anwendungen wie z. B. sendmail	98
4.5.7	IP-Adressen-Spoofing	100
4.5.8	ICMP-Angriffe	101
4.5.9	Internet-Routing-Angriffe	103
4.6	Zusammenfassung	104
5	Elemente eines Firewall-Systems	105
5.1	Aktive Firewall-Elemente	106
5.1.1	Architektur von aktiven Firewall-Elementen	106
5.1.2	Designkonzept aktiver Firewall-Elemente	109
5.2	Packet Filter	110
5.2.1	Allgemeine Arbeitsweise von Packet Filtern	111
5.2.2	Überprüfungen auf der Netzzugangsebene	113
5.2.3	Überprüfungen auf der Netzwerkebene	114
5.2.4	Überprüfungen auf der Transportebene	116
5.2.5	Strategien für den Aufbau und die Bewertung der Filterregeln	121
5.2.6	Beispiel für den Einsatz eines Packet Filters	121

5.2.7	Dynamischer Packet Filter	124
5.2.8	Benutzerorientierter Packet Filter	125
5.2.9	Sicherheitsrelevante Informationen in einem Packet Filter	129
5.2.10	Realisierungsformen für Packet Filter	131
5.2.11	Anwendungsgebiete von Packet Filtern	133
5.2.12	Zustandsorientierte Packet Filter	134
5.3	Application Gateway	136
5.3.1	Allgemeine Arbeitsweise des Application Gateway	137
5.3.2	Die Proxies	139
5.3.2.1	Application Level Proxies	139
5.3.2.2	SMTP Proxy	140
5.3.2.3	Benutzerorientierte Application Level Proxies	142
5.3.2.4	Telnet Proxy	144
5.3.2.5	FTP Proxy	149
5.3.2.6	HTTP Proxy	151
5.3.2.7	Authentication Proxy	154
5.3.2.8	Spezielle Proxies	154
5.3.2.9	Circuit Level Proxies	155
5.3.3	Anwendungsgebiete von Application Gateways	161
5.4	Security Management für aktive Firewall-Elemente	162
6	Konzepte für Firewall-Systeme	167
6.1	Ausschließlicher Einsatz eines Packet Filters	167
6.2	Ausschließlicher Einsatz eines Application Gateway	169
6.3	Kombination von Firewall-Elementen	171
6.3.1	Packet Filter und single-homed Application Gateway	173
6.3.2	Packet Filter und dual-homed Application Gateway	176
6.3.3	Zwei Packet Filter als Screened Subnet und ein single-homed Application Gateway	179
6.3.4	Zwei Packet Filter als Screened Subnet und ein dual-homed Application Gateway (High-level Security Firewall-System)	181
6.4	Möglichkeiten eines High-level Security Firewall-Systems	184
6.4.1	Internet Server	185
6.4.2	Intranet Server	187
6.4.3	Mehrere Application Gateways parallel	188
6.5	Das richtige Firewall-Konzept für jeden Einsatzfall	191
6.6	Mail-Konzept	192
6.7	DNS-Konzepte	194

7	Firewall-Systeme und Verschlüsselung	197
7.1	Sicherheitsmechanismen, die für die Verschlüsselung und die digitale Signatur notwendig sind	198
7.1.1	Private-Key-Verfahren	198
7.1.2	Public-Key-Verfahren	199
7.1.3	One-Way-Hashfunktion	200
7.1.4	Hybride Verschlüsselungstechnik	201
7.1.5	Zertifikations-Systeme	202
7.1.6	Chipkarte (SmartCard)	205
7.2	Objektorientierte Sicherheit: Verschlüsselung von Dokumenten und digitale Signatur	207
7.2.1	Briefumschlag und Signatur für die elektronische Post	208
7.2.1.1	Signatur eines Dokumentes	208
7.2.1.2	Verschlüsselung eines Dokuments	210
7.2.1.3	Prüfung der Vertrauenswürdigkeit des Dokuments und seine Entschlüsselung	211
7.2.1.4	Verifikation von Signaturen	213
7.2.2	Sicherheitsdienste des Sicherheitssystems	214
7.2.3	Die Digitale Signatur und die Objektverschlüsselung aus Sicht des Benutzers	214
7.2.4	Objektverschlüsselung und Firewall-Systeme	214
7.2.5	Der elektronische Vertrag: Die Rechtsform der Zukunft?	215
7.2.5.1	Sicherheitsvorteile	215
7.2.5.2	Risiken elektronischer Verträge	216
7.2.6	Unterschiedliche Konzepte zur Realisierung von objektorientierter Sicherheit	216
7.2.6.1	Privacy Enhanced Mail / PEM	217
7.2.6.2	Pretty Good Privacy / PGP	218
7.2.6.3	Abschließender Vergleich zwischen PEM und PGP	219
7.2.7	TeleTrusT Deutschland	220
7.2.8	MailTrusT-Projekt	221
7.3	Sicherheitssystem als transparente Lösung	221
7.3.1	Black-Box-Lösung	222
7.3.2	Security Sublayer im Endgerät: End-to-end-Verschlüsselung	224
7.3.3	Sicherheit in LAN-Segmenten	226
7.3.4	Kopplung von LAN-Segmenten mit einer Security Bridge	228
7.3.5	Kopplung von LAN-Segmenten über öffentliche Netze	229
7.3.6	Bildung von kryptographisch gesicherten logischen Netzen (VPN)	231
7.3.7	PC Security Komponente	233
7.3.8	Remote-Ankopplung	234
7.3.8.1	Kopplung von mobilen Rechnersystemen (Notebooks)	234

7.3.8.2	Kopplung von Heimarbeitsplätzen	235
7.3.9	Transparente Verschlüsselung und Firewall-Systeme	236
7.4	Vergleich zweier Konzepte: Transparente Sicherheit vs. Objektsicherheit	237
8	Authentikationsverfahren	239
8.1	Identifikation und Authentikation	239
8.2	Generelle Authentikationsverfahren	241
8.2.1	Paßwort-Verfahren	241
8.2.2	Einmal-Paßwort	242
8.2.3	Challenge-Response-Verfahren	243
8.3	Authentikationsverfahren für Firewall-Systeme	244
8.3.1	S/Key (MD5)	244
8.3.2	Authentikationsverfahren mit Security Token	247
8.3.3	Signaturkarte (Chipkarte)	249
9	Verschiedene Firewall-Lösungen und ihre Bewertung	253
9.1	Public Domain Software oder ein Firewallprodukt ?	253
9.1.1	Public Domain Software	253
9.1.2	Firewall-Produkte	255
9.2	Softwarelösung oder Turn-Key-Lösung ?	255
9.2.1	Was bietet eine Softwarelösung?	255
9.2.2	Was ist eine Turn-Key Lösung ?	257
9.3	Kriterien für die Beurteilung der tatsächlichen Sicherheitsleistung eines Firewall-Produktes	259
9.3.1	Offene und transparente Sicherheit	259
9.3.2	Geprüfte, nachweisbare Sicherheit	260
9.3.3	Sicherheit ohne staatliche Restriktionen	260
10	Praktischer Einsatz von Firewall-Systemen	261
10.1	Sichere Kopplung des eigenen Intranet an das Internet	263
10.2	Internet Server	265
10.3	Intranet Security	267
10.3.1	Höhere End-to-end-Sicherheit	269
10.3.2	Abschottung von Organisationseinheiten untereinander	270
10.3.3	Skalierbare Sicherheit	271
10.4	Externe Anbindung (Remote-Zugriff und Heimarbeitsplätze)	272

10.5	Ankopplung besonderer Organisationseinheiten	274
10.6	Externe Modem-Anschlüsse	275
10.7	Modem-Verbindungen aus dem unsicheren Netz in das zu schützende Netz	277
10.8	Virengefahr	279
10.8.1	Integration von Viren-Scannern am Common Point of Trust	280
10.8.2	Weitere technische, personelle und organisatorische Maßnahmen	285
11	Ein Firewall-System ist mehr als ein Produkt	287
11.1	Firewall-Sicherheitspolitik	287
11.1.1	Sicherheitsziele	288
11.1.2	Darstellung der zu schützenden Ressourcen	289
11.1.3	Festlegung von Kommunikationsanforderungen	290
11.1.4	Festlegung von Diensten und Anwendungen	291
11.2	Zusätzliche Sicherheitsmaßnahmen	294
11.2.1	Infrastruktur	294
11.2.2	Organisation	296
11.2.2.1	Technische Realisierung	296
11.2.2.2	Security Management	296
11.2.2.3	Benutzer	300
11.2.2.4	Allgemeine Sicherheitsmaßnahmen	300
11.2.3	Personal	301
11.2.3.1	Security Management	301
11.2.3.2	Benutzer	303
11.2.4	Notfall	305
11.3	Grenzen eines Firewall-Systems	305
11.3.1	Hintertüren	305
11.3.2	Interne Angriffe	306
11.3.3	Anwendungsdatenorientierte Angriffe	306
11.3.4	Eine richtige Sicherheitspolitik und richtige Umsetzung der Sicherheitpolitik	306
11.3.5	Trittbrettfahrer	307
12	Besondere Aufgabenstellungen bei der Verwendung von Firewall-Systemen	309
12.1	Network Address Translation	309
12.1.1	Firewall-System und Network Address Translation	311
12.1.2	Probleme für Netze, die mit illegalen IP-Adressen arbeiten	312
12.2	Domainen-Namen	313

12.3	Verwaltung mehrerer Firewall-Systeme mit Hilfe eines Security Managements	313
12.4	Geschachtelte Firewall-Konstellationen	314
12.5	Ausfallsicherheit	315
13	Weiterführende Aufgabenstellungen beim Einsatz von Firewall-Systemen	317
13.1	Logbuch – Belastung oder Nutzen ?	317
13.1.1	Ziele der Protokollierung	317
13.1.1.1	Erkennung von Sicherheitsverletzungen	317
13.1.1.2	Beweissicherung der Handlungen von Benutzern	318
13.1.2	Protokollierung von Ereignissen	318
13.1.3	Erkennen von Sicherheitsverletzungen durch die Auswertung von Protokolldaten der Logbücher	320
13.1.3.1	Erkennen von bekannten sicherheitsrelevanten Aktionen	320
13.1.3.2	Erkennen von Anomalien	322
13.1.3.3	Vergleich der verschiedenen Auswertungskonzepte zur Erkennung von Sicherheitsverletzungen	323
13.1.4	Alarmierung	325
13.1.5	Beweissicherung	325
13.1.6	Schutz der Protokolldaten	326
13.1.7	Reaktionen auf eine Sicherheitsverletzung	327
13.1.8	Datenschutzaspekte	329
13.2	Java und ActiveX	330
13.2.1	Java	333
13.2.2	ActiveX	337
13.3	Anschaffung und Betrieb eines Firewall-Systems	338
13.3.1	Beschaffungsphase eines Firewall-Systems	339
13.3.1.1	Aufwand für die Beschaffungsphase	339
13.3.1.2	Installationsphase eines Firewall-Systems	340
13.3.2	Aufrechterhaltung des Betriebs eines Firewall-Systems	341
13.3.2.1	Rechteverwaltung	341
13.3.2.2	Analyse der Logbuchdaten	342
13.3.2.3	Einrichtung neuer Dienste	342
13.3.2.4	Genereller administrativer Aufwand für das Firewall-System	342
13.3.2.5	Auswertung der Logbuchdaten auf dem Security Management	343
13.3.2.6	Sicherer Betrieb eines Firewall-Systems	343
13.3.3	Zusammenfassung der Kosten	345
13.4	Evaluierung und Zertifizierung von Firewall-Systemen	346

13.4.1	ITSEC-Zertifizierung	346
13.4.2	NCSA-Zertifizierung	355
13.5	Weiterentwicklung von Firewall-Systemen	359
13.5.1	Höhere Geschwindigkeiten	359
13.5.2	Identifikations- und Authentifikationsverfahren	359
13.5.3	Neue Proxies für neue Dienste	360
13.5.4	Protokollauswertung	360
14	Recht im Internet	361
14.1	Aktuelle Formen des Delikts »Computerkriminalität«	362
14.1.1	Persönlichkeitsrechtsverletzungen	362
14.1.2	Wirtschaftsdelikte	363
14.1.2.1	Computermanipulationen	363
14.1.2.2	Computersabotage und -erpressung	364
14.1.2.3	Hacker	364
14.1.2.4	Wirtschaftsspionage	364
14.1.2.5	Softwarediebstahl und andere Formen der Produktpiraterie	365
14.1.3	Sonstige Delikte	365
14.2	Rechtsfragen	365
14.3	Paradigmenwechsel und Perspektiven	366
	Gesellschaftliche Veränderungen	366
14.4	Zusammenfassung	368
A	Anhang A: Sicherheitsstandards	369
B	Anhang B: Wichtige Adressen	377
C	Anhang C: Legende	379
D	Anhang D: Firewall-Produkte	381
E	Anhang E: Literaturverzeichnis	383
F	Anhang F: Sicherheitsanforderungen an Internet-Firewalls (BSI)	387
F.1	Einleitung	387
F.2	Gefährdungen bei der Benutzung des Internet	388
F.2.1	Vielfalt der Netzdienste	388
F.2.2	Verlust der Vertraulichkeit und Integrität	389

F.2.3	Konzeptionsfehler	389
F.2.4	Mißbrauch von frei verfügbaren Informationen	391
F.3	Schutzmöglichkeiten	391
F.4	Forderungen an Firewalls	393
F.4.1	Forderungen zur Abwehr von Angriffen auf die Firewall-Anordnung	394
F.4.2	Forderungen zur Abwehr von Angriffen aus dem Internet auf das zu sichernde Netz	396
F.4.3	Organisatorische Maßnahmen	401
F.5	Adressen	403
F.6	Literatur	404
G	Anhang G: Glossar, Abkürzungen	405
	Index	415