

Inhaltsverzeichnis

	Für wen ist das Buch geschrieben?	11
I	Was ist eine Firewall?	13
1.1	IT-Sicherheitskonzept	19
1.2	Abnahme der Firewall	20
1.3	Zusammenfassung:	22
2	Überblick über die verschiedenen Firewall-Technologien	23
2.1	OSI-Modell (OSI: Open System Integration)	23
2.2	Hardware-Adresse	25
2.3	IP-Adresse	26
2.4	Router	29
2.5	TCP und UDP	31
2.6	Paketfilter	36
2.7	Proxy	41
2.8	Hybride Firewalls	45
2.9	Transparenter Proxy (Second-Generation Application-Level Firewall)	45
2.10	IDS (Intrusion Detection System)	45
2.11	Zusammenfassung	46
3	Check Points Firewall bzw. die Stateful Inspection Technology	47
3.1	Vergleich Paketfilter, Proxy und Stateful Inspection	50
3.2	Architektur der Stateful Inspection	51
3.3	Zusammenfassung	56
4	Produkte und Module von Check Point	57
4.1	Begriffserklärung FireWall-I/VPN-I	57
4.2	Leistungsmerkmale der FireWall-I/VPN-I 4.1 und NG	57
4.3	Plattformen und Systemvoraussetzungen	59
4.4	Leistungsumfang der FireWall-I/VPN-I-Module	60
4.5	Leistungsumfang der VPN-I-Module	62
4.6	Weitere Produkte von Check Point	63

4.7	Neue Produktleistungsmerkmale	66
4.8	Zusammenfassung	69
5	Kostenaspekte	71
5.1	Allgemeines	71
5.2	Anforderungen eines anspruchsvollen Sicherheitskonzepts an die Firewall	71
5.3	Weitere Kostenaspekte	73
5.4	Software-Kosten Firewall-1/VPN-1	74
5.5	Beispielkonfiguration	79
5.6	Zusammenfassung	82
6	FireWall-1-(Standalone)-Installation und -Konfiguration	83
6.1	Auswahl der Plattform	83
6.2	Installation FireWall-1 4.1 auf Windows NT	84
6.3	Installation FireWall NG auf Windows 2000	99
6.4	Installation FireWall-1 NG auf Linux	114
6.5	Zusammenfassung	124
7	Beschreibung und Benutzung der FireWall-1 GUIs	125
7.1	GUI der FireWall-1 & VPN-1 Version 4.1	125
7.2	GUI der FireWall-1 & VPN-1-Version 5.0 (FP 1 und FP 2)	134
7.3	GUI der FireWall-1 & VPN-1 Version 5.0 (FP 3)	142
7.4	Zusammenfassung	147
8	Definition von Filterregeln, Netzwerkobjekten und Diensten	149
8.1	Allgemeines	149
8.2	Erstellung einer neuen Security-Policy über den Vorlagen-Manager (Version 4.1)	150
8.3	Elemente der Filterregeln (Version 4.1)	152
8.4	Die Definition von Netzwerkobjekten (Version 4.1)	158
8.5	Definition von Netzwerkdiensten	169
8.6	Objektdefinition und Filterregeln für unser Beispiel	176
8.7	Definition von Filterregeln, Netzwerkobjekten und Diensten bei der NG-Version	181
8.8	Anmerkungen zum Boot der FireWall-1	197
8.9	Zusammenfassung	197

9	Sicherheitsgrundeinstellungen (Security Policy Properties)	199
9.1	Sicherheitsgrundeinstellungen Version 4.1	199
9.2	Sicherheitsgrundeinstellungen bei NG	215
9.3	Zusammenfassung:	228
10	Authentisierung	229
10.1	Durch die FireWall-1 (4.1 und NG) unterstützte Authentisierungstypen	229
10.2	Vergleich der verschiedenen Authentisierungsverfahren	236
10.3	Konfiguration der verschiedenen Authentisierungsverfahren (4.1 und NG)	236
10.4	Sicherheitsgrundeinstellungen	252
10.5	Das Problem der »nicht ausreichenden Informationen«	254
10.6	Beispiel	255
10.7	Zusammenfassung:	260
11	NAT: Network Address Translation	261
11.1	Einführung	261
11.2	Funktion von NAT	262
11.3	Wie hat Check Point NAT und PAT realisiert?	267
11.4	NAT-Beispiele für die FireWall-1	275
11.5	Zusammenfassung	287
12	Security-Server, URL-Filter, Virens Scanner	289
12.1	Allgemeines	289
12.2	Konfiguration FTP-Security-Server	293
12.3	Konfiguration HTTP-Security-Server	303
12.4	Konfiguration SMTP-Security-Server	323
12.5	TCP-Ressourcen (NG)	335
12.6	Zusammenfassung	338
13	Verschlüsselung	339
13.1	Einführung in die Verschlüsselungstechniken	339
13.2	Symmetrische Verschlüsselung	341
13.3	Asymmetrische Verschlüsselung	343
13.4	Trust Center und die digitale Signatur	347
13.5	IPsec	349
13.6	Schlüsselmanagement-Protokolle	355
13.7	Zusammenfassung	356

14	VPN-I-Installation und -Konfiguration	357
14.1	Was ist ein VPN?	357
14.2	Vergleich zwischen VPN-Lösungen und traditionellen Unternehmensnetzen	357
14.3	Check Points VPN-I	361
14.4	Installation Konfiguration VPN-I (Version 4.1)	362
14.5	Installation und Konfiguration VPN-I Version NG	382
14.6	Zusammenfassung	401
15	SecuRemote und SecureClient	403
15.1	Allgemeines	403
15.2	Leistungsumfang von SecuRemote und SecureClient Version 4.1 und NG	405
15.3	Architektur SecuRemote und SecureClient	406
15.4	Installation und Konfiguration von SecuRemote Version 4.1	407
15.5	Installation und Konfiguration von SecuRemote, SecureClient Version NG	416
15.6	Zusammenfassung	429
16	Traffic-Management und FloodGate-I	431
16.1	Was ist Traffic-Management?	431
16.2	Was ist Quality of Service?	432
16.3	Traffic-Management und IP-Anwendungen	434
16.4	Produkteigenschaften FloodGate-I	441
16.5	FloodGate-I-Installation Version 4.1	443
16.6	FloodGate-I-Konfiguration Version 4.1	444
16.7	FloodGate-I Version NG	455
16.8	Zusammenfassung	461
A	Glossar und Abkürzungsverzeichnis	463
	Stichwortverzeichnis	487