

Inhaltsverzeichnis

1	Einleitung	13
2	Grundlagen	17
2.1	Entwicklung und Verbreitung des Internets und TCP/IP	18
2.1.1	Entstehung des Internets	19
2.1.2	Kommerzialisierung des Internets	26
2.1.3	Heutige Verbreitung des Internets	28
2.2	Grundlagen von TCP/IP	30
2.2.1	Die Schichtenmodelle	31
2.2.2	Netzwerkschicht	33
2.2.3	Internetschicht	34
2.2.4	Transportschicht	53
2.2.5	Weitere Protokolle des IP	61
2.2.6	Applikationsschicht	66
2.3	Die Offenheit der Protokolle und das Gefahrenpotential	68
2.4	Einsatz von Firewalls zum Schutz vertrauenswürdiger Netzwerke	74
2.5	De-militarisierte Zone	77
3	Technische Sicherheitsmechanismen	81
3.1	Paketfilter	82
3.1.1	Vorteile von Paketfiltern	83
3.1.2	Nachteile von Paketfiltern	83
3.2	Circuit Level und Application Level Gateways	92
3.2.1	Vorteile von Circuit Level und Application Level Gateways	95
3.2.2	Nachteile von Circuit Level und Application Level Gateways	96
3.3	Stateful Inspection	97
3.3.1	Vorteile der Stateful Inspection	98
3.3.2	Nachteile der Stateful Inspection	99
4	Das Sicherheitskonzept	103
4.1	Allgemeines zum Sicherheitskonzept	104
4.2	Planung und Entwicklung des Sicherheitskonzepts	105
4.2.1	Schaffung der Grundvoraussetzungen	106
4.2.2	Feststellung des Ist-Zustands	107
4.2.3	Definition von Prioritäten	108
4.2.4	Schützenswerte Güter	110
4.2.5	Mögliche Risiken und Bedrohungen	111

4.2.6	Bewertung der Bedrohungen und Risiken	114
4.2.7	Kosten-Nutzen Analyse und das Sicherheitsniveau	115
4.2.8	Festlegung und Beurteilung von Maßnahmen für die verschiedenen Bereiche	119
4.2.9	Sicherheitskonzept	123
4.2.10	Umsetzung der Maßnahmen	126
4.2.11	Dokumentation des Sicherheitsniveaus und der Maßnahmen	131
4.3	Aufrechterhaltung der Sicherheit	132
4.3.1	Notwendige Maßnahmen zur Erhaltung der Sicherheit	132
4.3.2	Überprüfung des Sicherheitsniveaus auf der organisatorischen Ebene ..	134
4.3.3	Überprüfung des Sicherheitsniveaus auf der technischen Ebene	136
4.3.4	Einige Hinweise zur Überprüfung einer FireWall-1	144
5	Check Point FireWall-1 Grundlagen und Installation ...	147
5.1	Komponenten der Check Point FireWall-1	147
5.1.1	Inspektions-Modul	148
5.1.2	Managementmodul	150
5.1.3	Das GUI	151
5.2	Einige optionale Möglichkeiten der Check Point FireWall-1 ...	159
5.2.1	Remote-Management	160
5.2.2	Authentisierung	163
5.2.3	Virtual Private Networks	164
5.2.4	Load Balancing	166
5.2.5	Routerverwaltung mit dem Open Security Manager	167
5.2.6	Integration weiterer Software	168
5.3	Leistungsfähigkeit der Check Point FireWall-1	170
5.4	Installation und De-Installation	174
5.4.1	Installationsvoraussetzungen	174
5.4.2	Absicherung von Microsoft Windows NT	176
5.4.3	Installation unter Microsoft Windows NT	180
5.4.4	Installation und Absicherung von Sun Solaris	206
5.4.5	Installation unter Sun Solaris	219
5.4.6	Installation und Absicherung von Linux	232
5.4.7	Hinweise zur Installation der FW-1 unter anderen Betriebssystemen ...	243
5.4.8	De-Installation der Check Point FireWall-1	249
5.4.9	Upgrade von Version 3.x	250
5.4.10	Upgrade von Version 4.0 auf 4.1	251
5.4.11	Installation von Service Packs	253
5.5	Lizenzierung der Check Point FireWall-1	256
5.5.1	Lizenztypen	258
5.5.2	Eingabe von Lizenzen	264
5.5.3	Features einer FireWall-1-Lizenz	268
5.5.4	Kontrolle eingegebener Lizenzen	273
6	Regelbasiseditor	275
6.1	Das Menü und die Werkzeugleiste	276
6.1.1	Die Werkzeugleiste des Regelbasiseditors	276
6.1.2	Kurze Vorstellung der einzelnen Menüs	277
6.1.3	Die Grundeinstellungen einer FireWall-1	307
6.2	Installation einer Regelbasis	362



7	Manager der FireWall-1	363
7.1	Netzwerkobjekt-Manager	363
7.1.1	Workstation	364
7.1.2	Network	394
7.1.3	Domain	398
7.1.4	Router	400
7.1.5	Switch	418
7.1.6	Integrated Firewall	422
7.1.7	Group	434
7.1.8	Logical Server	435
7.1.9	Address Range	441
7.1.10	Gateway Cluster	442
7.2	Service-Manager	445
7.2.1	TCP	447
7.2.2	Compound TCP	449
7.2.3	UDP	450
7.2.4	RPC	451
7.2.5	ICMP	452
7.2.6	Other	455
7.2.7	Group	457
7.2.8	Port Range	459
7.3	Ressourcen-Manager	460
7.3.1	URI	461
7.3.2	URI for Traffic Control	475
7.3.3	SMTP	476
7.3.4	FTP	485
7.3.5	Group	489
7.4	Server-Manager	491
7.4.1	UFP-Server	492
7.4.2	CVP-Server	494
7.4.3	RADIUS und Gruppe von RADIUS-Servern	496
7.4.4	TACACS-Server	498
7.4.5	Defender-Server	500
7.4.6	LDAP-Server	502
7.4.7	CA (ab Version 4.1)	509
7.4.8	Policy-Server (ab Version 4.1)	512
7.5	User-Manager	513
7.5.1	Group	515
7.5.2	External Group	517
7.5.3	Template	518
7.5.4	Anlegen eines Benutzers	519
7.6	Zeit-Manager	531
7.6.1	Time	532
7.6.2	Group	534
7.7	Key-Manager	535
7.7.1	SPI	536

8	Eingabe von Regeln	539
8.1	Allgemeines	539
8.2	Angabe von Absender und Ziel	542
8.3	Auswahl an Services	544
8.4	Geforderte Aktionen: Action	545
8.4.1	Accept	546
8.4.2	Drop	547
8.4.3	Reject	547
8.4.4	User Auth	548
8.4.5	Client Auth	549
8.4.6	Session Auth	549
8.4.7	Encrypt	550
8.4.8	Client Encrypt	550
8.5	Die Reaktion der Firewall: Track	550
8.5.1	No	551
8.5.2	Short	551
8.5.3	Long	552
8.5.4	Account	552
8.5.5	Alert	552
8.5.6	Mail	553
8.5.7	SNMP Trap	553
8.5.8	UserDefined	553
8.6	Installationsmöglichkeiten – Install on...	554
8.6.1	Gateways	554
8.6.2	Source	554
8.6.3	Destination	555
8.6.4	Routers	555
8.6.5	Integrated Firewalls	556
8.6.6	Targets	556
8.6.7	Hinweise	558
8.7	Zeitliche Beschränkung von Regeln: Time	560
8.8	Stealth-Regel	561
8.9	Clean-up-Regel	562
8.10	Reihenfolge, in der die Regeln greifen	563
8.11	Weiteres	567
9	System-Status und Log Viewer	569
9.1	Beschreibung des System Status	569
9.1.1	Grundsätzliches	569
9.1.2	Zustände des System-Status	573
9.1.3	Das Menü und die Werkzeugleiste	575
9.1.4	Eingabe von Alarmen bei Statuswechsel	576
9.2	Beschreibung des Log Viewers	578
9.2.1	Allgemeine Einstellungen und Hinweise	578
9.2.2	Die Werkzeugleiste und Menüs	581
9.2.3	Log-Einträge	587
9.2.4	Klassisches Log: Security Log	595
9.2.5	Accounting-Log	597
9.2.6	Log aktiver Verbindungen	598
9.2.7	Block-Intruder-Funktionalität	599

10	Authentisierung mit der FireWall-1	605
10.1	Authentisierungsmethoden der FireWall-1	606
10.1.1	Interne Authentisierungsmethoden	606
10.1.2	Externe Authentisierungsmethoden	614
10.2	Authentisierung von Benutzern	621
10.2.1	User-Authentisierung	622
10.2.2	Client-Authentisierung	628
10.2.3	Session-Authentisierung	639
10.2.4	Kombination der Authentisierungsverfahren	645
10.2.5	Reihenfolge der Regeln zur Authentisierung	646
10.2.6	Hinweise zur Einrichtung	647
10.3	Anwendung von Account Units	654
10.3.1	LDAP – Lightweight Directory Access Protocol	655
10.3.2	Installation des Account Management Client	660
10.3.3	Vorbereitungen an der FireWall-1	662
10.3.4	Einrichtung und Verwaltung von Benutzern auf LDAP-Servern	667
10.3.5	Nutzung der Authentisierungsmöglichkeit in einer Regelbasis	681
11	Network Address Translation	685
11.1	Notwendigkeit und Möglichkeiten	685
11.1.1	RfC 1918	685
11.1.2	Prinzip der NAT	689
11.2	Static Mode	689
11.2.1	Static Destination Mode	690
11.2.2	Static Source Mode	691
11.3	Hide Mode	692
11.4	Einrichtung der NAT bei einer FireWall-1	696
11.4.1	Das NAT-GUI	696
11.4.2	Automatische NAT	698
11.4.3	Manuelle NAT	701
11.5	Mögliche Probleme bei der NAT	707
11.5.1	ARP	707
11.5.2	Routing	710
11.5.3	Host-Routing	711
11.5.4	Anti-Spoofing	713
11.5.5	Mögliche Probleme mit einzelnen Protokollen	714
12	Virtual Private Networks (VPN) mit der VPN-1/FireWall-1	717
12.1	Grundlagen der Kryptographie	718
12.1.1	Grundsätzliche Forderungen an Kryptosysteme	719
12.1.2	Angriffe gegen Verschlüsselungssysteme	721
12.1.3	Verschlüsselungsalgorithmen	724
12.1.4	Symmetrische Verschlüsselung	725
12.1.5	Echtheitsbestätigung übertragener Daten	738
12.1.6	Verschlüsselungsprotokolle	750
12.2	Anwendbare Möglichkeiten in der VPN-1	752
12.3	Verschiedene Typen von VPN	753

12.3.1	Intranet VPN	753
12.3.2	Remote-Access VPN	754
12.3.3	Extranet VPN	754
12.3.4	Vollständiges VPN	755
12.4	VPN von Firewall zu Firewall	756
12.4.1	FWZ	756
12.4.2	IKE	760
12.4.3	Manual IPSEC	773
12.4.4	SKIP	774
12.5	VPN von SecuRemote-Clients zur FireWall-1	776
12.5.1	Das Prinzip von SecuRemote	776
12.5.2	Installation von SecuRemote auf einem PC	779
12.5.3	Einrichtung der VPN-1 für die Nutzung von SecuRemote	783
12.5.4	Einrichtung von SecuRemote und der laufende Betrieb	785
12.6	Der Einsatz von SecureClients	790
12.6.1	Restrisiken bei der Nutzung von SecuRemote	790
12.6.2	Der Policy-Server	791
12.6.3	Installation des SecureClient	792
12.6.4	Absicherung von Rechnern durch SecureClient	793
12.6.5	Secure-Client in der Praxis	795
12.7	Hinweise zur Konfiguration von SecuRemote und Secure-Client	797
12.7.1	Einrichtung vieler SecuRemote-Clients	798
12.7.2	Authentisierung mit dem Hybrid Mode	798
12.7.3	Nutzung des Nameservice im Intra- und Internet	800
12.7.4	Ausfallsicherheit für SecuRemote und Secure-Client	804
12.7.5	Die Konfigurationsdatei »userc.C«	804
13	Ausfallsicherheit mit der VPN-1/FireWall-1	807
13.1	Überlappende Verschlüsselungsdomeins	808
13.1.1	Full overlap – Volle Überschneidung der Verschlüsselungsdomeins	808
13.1.2	Partial overlap – Teilweise Überschneidung der Verschlüsselungsdomeins	809
13.1.3	Proper subset – Saubere Teilmengen von Verschlüsselungsdomeins	810
13.2	Hochverfügbarkeitslösung für eine Firewall – Single Entry Point: SEP	812
13.2.1	Prinzipielle Arbeitsweise eines SEP	812
13.2.2	Grundkonfiguration der einzelnen Maschinen	813
13.2.3	Einrichtung des SEP über das GUI	816
13.2.4	Einrichtung der Synchronisation von State Tables	817
13.2.5	Einschränkungen von SEP	818
13.3	Ausfallsicherheit für SecuRemote – Multiple Entry Points: MEP	819
13.3.1	Das Prinzip von MEP	820
13.3.2	Die Konfiguration von MEP und Einrichtung von IP-Pools	821
13.3.3	Einschränkungen von MEP	825

14	Bedienung über die Kommandozeile	827
14.1	Basiskommandos	827
14.2	Das Kommando fw	833
14.2.1	Allgemeiner Aufbau	833
14.2.2	Kommandos für die Lizenzverwaltung	834
14.2.3	Kommandos für das Monitoring	838
14.2.4	Kommandos für die Konfiguration	846
14.2.5	Kommandos für die Benutzerverwaltung von Hand	851
14.2.6	Verwaltung von Zertifikaten und der internen CA	860
14.2.7	Kommandos für die Accelerator Card	862
14.2.8	Weitere Kommandos der FireWall-1	863
14.3	Beispiel: Installation und De-Installation der Regelbasis von Hand	869
14.4	Die Sprache INSPECT	871
15	Praktische Konfigurationsbeispiele für die FireWall-1	873
15.1	Hinweis zur Vergabe von Namen	873
15.2	Vorstellung einer Beispielumgebung	876
15.3	Aufbau einer einfachen Regelbasis	877
15.3.1	Reihenfolge der Regeln	877
15.3.2	Anpassung der Grundeinstellungen der FireWall-1	879
15.3.3	Spezielle Regeln	880
15.4	Nutzung von Ressourcen	883
15.4.1	Ressourcen für SMTP	885
15.4.2	Ressourcen für FTP	887
15.4.3	Ressourcen für HTTP	888
15.4.4	Definition eigener Ressourcen	892
15.4.5	Einige mögliche Probleme bei FTP, HTTP und SMTP	894
15.5	Einbindung und Konfiguration von Alarmen	897
15.6	Authentisierung von Benutzern für verschiedene Dienste	900
15.6.1	Eingabe von Regeln zur Authentisierung	900
15.6.2	User-Authentisierung für Telnet und HTTP	902
15.6.3	User-Authentisierung für HTTP über SSL	904
15.6.4	User-Authentisierung für FTP	907
15.6.5	Client-Authentisierung	908
15.6.6	Session-Authentisierung	910
15.7	Einrichtung von NAT	912
15.7.1	Static Mode	912
15.7.2	Hide Mode	914
15.8	Remote Management der FireWall-1	915
15.8.1	Abheben des GUI	916
15.8.2	Trennung von Inspektions- und Management-Modul	917
15.9	Routerverwaltung mit der FireWall-1	923
15.9.1	Grundvoraussetzungen, Regeln und deren Installation	923
15.9.2	Import der ACLs von einem Router	928

15.10	Aufbau Virtueller Privater Netzwerke	931
15.10.1	Aufbau eines festen VPN mit FWZ	932
15.10.2	Aufbau eines festen VPN mit SKIP	937
15.10.3	Aufbau eines festen VPN mit Manual IPSEC	944
15.10.4	Aufbau eines festen VPN mit IKE	948
15.11	Sichere Datenübertragung mit SecuRemote und Secure-Client	954
15.11.1	Vorbereitung der VPN-1 am Netzwerk des Unternehmens	955
15.11.2	Installation und Einrichtung auf der Client-Seite	956
15.11.3	Definition der Regelbasis	957
15.11.4	Betrieb des VPN	958
15.12	Load-Balancing	959
15.12.1	Load-Balancing für HTTP	959
15.12.2	Load-Balancing für FTP und andere Dienste	960
15.13	Synchronisation mehrerer FireWall-1	962
15.14	Performance-Tuning an einer FireWall-1/VPN-1	963
15.14.1	Einige Bemerkungen zu Hardware und Betriebssystemen	964
15.14.2	Einige Bemerkungen zur Konfiguration der FireWall-1/VPN-1	967
A	Weitere Quellen über Check Point FireWall-1	973
A.1	Literatur	973
A.2	Internet	975
A.2.1	Web-Server	975
A.2.2	Mailinglisten	977
A.2.3	News-Server	981
B	Verzeichnisse	983
B.1	Verzeichnis von Ports einer VPN-1 & FireWall-1	983
B.2	Verzeichnisse von TCP- und UDP-Ports	985
C	Glossar	987
	Stichwortverzeichnis	1011