

INHALT

1 Vorwort.....	14
2 Grundlagen.....	19
2.1 Entwicklung und Verbreitung des Internets und TCP/IP	20
2.2 Grundlagen von TCP/IP	30
2.3 Die Offenheit der Protokolle und das Gefahrenpotential	63
2.4 Firewalls zum Schutz vertrauenswürdiger Netzwerke	68
2.5 De-militarisierte Zone.....	71
3 Technische Sicherheitsmechanismen.....	75
3.1 Paketfilter	76
3.2 Circuit Level und Application Level Gateways	85
3.3 Stateful Inspection	90
4 Das Sicherheitskonzept.....	95
4.1 Allgemeines zum Sicherheitskonzept.....	96
4.2 Planung und Entwicklung des Sicherheitskonzepts.....	97
4.3 Aufrechterhaltung und Überprüfung der Sicherheit	120
5 Grundlagen von Check Point NG.....	135
5.1 Secure Virtual Networking / Secure Internal Communication	135
5.2 Die Basiskomponenten	137
5.2.1 Inspektions-Modul	139
5.2.2 SmartCenter – das Management-Modul.....	141
5.2.3 SmartConsole – das GUI.....	142
5.2.4 Begriffliches.....	153
5.3 Optionale Möglichkeiten der Check Point Next Generation....	156
5.4 Leistungsfähigkeit von Check Point Next Generation	167
5.5 Übersicht zu Grundausrüstung und Zubehör	170
6 Installation und Lizenzierung	175
6.1 Installationsplattformen und -anforderungen	175
6.2 Absicherung des Betriebssystems.....	177
6.2.1 Microsoft Windows NT Server	177
6.2.2 Microsoft Windows 2000 Server.....	180
6.2.3 Sun Solaris	183
6.2.4 Red Hat Linux.....	193
6.3 Installation von Check Point NG unter Windows	203
6.3.1 Installation eines Firewall-Moduls	207

6.3.2	Installation des Management-Moduls.....	213
6.3.3	Installation der SmartConsole	218
6.4	Installation von Check Point NG unter Unix.....	221
6.5	Check Point Appliances.....	225
6.6	SecurePlatform.....	227
6.7	De-Installation von Next Generation.....	230
6.8	Migration von Version 4.x zu Next Generation.....	231
6.8.1	Grundsätzliches zum Upgrade	231
6.8.2	Upgrade zu Next Generation Feature Pack 1 von Hand	234
6.8.3	Upgrade mit Skripten	237
6.8.4	Automatisches Upgrade auf NG ab Feature Pack 3	247
6.9	Installation von Feature Packs	247
6.10	Lizenzierung und Lizenzverwaltung	250
6.10.1	Lizenztypen.....	252
6.10.2	Bezeichnung der unterschiedlichen Lizenztypen.....	257
6.10.3	Eingabe von Lizenzen	266
7	SmartDashBoard (Policy Editor).....	269
7.1	Objektbaum, Regelsätze und SmartMap.....	270
7.2	Das Menü und die Werkzeugleiste	272
7.2.1	Die Werkzeugleiste des SmartDashboard.....	272
7.2.2	Kurze Vorstellung der einzelnen Menüs	273
7.3	Die Grundeinstellungen von NG	293
7.3.1	Allgemeines.....	293
7.3.2	FireWall-1	294
7.3.3	NAT – Network Address Translation.....	308
7.3.4	Authentication.....	310
7.3.5	VPN-1 Pro	313
7.3.6	VPN-1 Net.....	318
7.3.7	Remote Access	320
7.3.8	Extranet Management Interface.....	332
7.3.9	LDAP Account Management	333
7.3.10	FloodGate-1	335
7.3.11	SmartMap.....	337
7.3.12	Management High Availability	338
7.3.13	ConnectControl	339
7.3.14	OSE – Open Security Extension.....	341
7.3.15	Stateful Inspection.....	344
7.3.16	Profile Based Management.....	347
7.3.17	Log and Alert	347
7.3.18	Logging Modifiers	349
7.3.19	OPSEC.....	353
7.3.20	SmartCenter Access.....	354
7.3.21	Non Unique IP Addresses	356
7.3.22	SmartDashboard Customization.....	357
7.4	Überprüfung und Installation einer Regelbasis	359

8 Objektmanagement in NG.....	361
8.1 Allgemeines	362
8.2 Netzwerkobjekte	363
8.2.1 Check Point	366
8.2.2 Node.....	370
8.2.3 Interoperable Device	372
8.2.4 Übergreifende Eigenschaften von Check Points, Nodes und Interoperable Device	373
8.2.5 Network	441
8.2.6 Domain.....	444
8.2.7 OSE Device	446
8.2.8 Group	459
8.2.9 Logical Server	462
8.2.10 Address Range.....	468
8.2.11 Dynamic Object	469
8.2.12 VoIP Domains.....	470
8.3 Services	474
8.3.1 TCP	475
8.3.2 Compound TCP.....	478
8.3.3 Citrix TCP	479
8.3.4 UDP	479
8.3.5 RPC	482
8.3.6 ICMP	483
8.3.7 Other	484
8.3.8 Group	487
8.3.9 DCE-RPC	488
8.4 Ressourcen – Resources	488
8.4.1 URI	490
8.4.2 URI for QoS	505
8.4.3 SMTP.....	506
8.4.4 FTP	517
8.4.5 TCP	521
8.4.6 CIFS.....	522
8.5 OPSEC-Applikationen – OPSEC Applications	524
8.5.1 OPSEC-Application	524
8.5.2 CVP Group.....	531
8.5.3 UFP Group.....	534
8.5.4 CPMI Group.....	535
8.6 Server	537
8.6.1 RADIUS und Gruppe von RADIUS-Servern	537
8.6.2 TACACS.....	540
8.6.3 LDAP Account Unit	541
8.6.4 Certificate Authority	550
8.6.5 SecuRemote DNS.....	554
8.7 Benutzer und Administratoren – Users and Administrators ...	556
8.7.1 Anlegen von Benutzern und Benutzergruppen	557
8.7.2 Anlegen von Benutzergruppen	570

8.7.3	Anlegen von Administratoren und Gruppen	572
8.7.4	Externe Benutzerprofile	578
8.7.5	Templates	582
8.8	Berechtigungsprofile – Permission Profiles	583
8.9	Zeiten – Time	586
8.9.1	Time	587
8.9.2	Group	589
8.9.3	Scheduled Event	590
8.10	VPNs – VPN Communities	591
8.10.1	Site-to-Site – Intranet	592
8.10.2	Partner – Extranet	602
8.10.3	Remote Access	606
8.11	Remote Access – Connection Profile	609
8.12	QoS – Quality of Service Classes	612
8.12.1	DiffServ Class of Service	612
8.12.2	Low Latency Class of Service	613
8.12.3	DiffServ Class of Service Group	613
8.13	SmartView Monitor – Virtual Links	614
8.14	UserAuthority – Credential Manager	616
8.14.1	UA Authentication Domains	618
8.14.2	Operations	619
8.14.3	Trusts	621
9	<i>Eingabe von Regeln</i>	<i>623</i>
9.1	Allgemeines	624
9.2	Eingabe von Absender und Ziel	627
9.3	Die Spalte VPN	628
9.4	Auswahl an Services oder Ressourcen	630
9.5	Geforderte Aktionen: Action	631
9.5.1	Accept	632
9.5.2	Drop	633
9.5.3	Reject	633
9.5.4	User Auth	634
9.5.5	Client Auth	634
9.5.6	Session Auth	635
9.5.7	Encrypt	635
9.5.8	Client Encrypt	636
9.6	Die Reaktion der Firewall: Track	636
9.6.1	None	637
9.6.2	Log	637
9.6.3	Account	637
9.6.4	Alarmierung	638
9.7	Installationsmöglichkeiten: Install On	638
9.7.1	Policy Targets	639
9.7.2	Gateways	640
9.7.3	Destination	640
9.7.4	Source	640

9.7.5	OSE-Devices.....	640
9.7.6	Embedded Device	641
9.7.7	Targets.....	641
9.8	Zeitliche Beschränkung von Regeln: Time.....	642
9.9	Stealth-Regel.....	642
9.10	Clean-up-Regel.....	643
9.11	Reihenfolge, in der die Regeln greifen	644
9.12	Regeln verstecken.....	648
9.13	(Temporäres) Ausschalten von Regeln.....	648
9.14	Anfragen an die Regelbasis mit Queries.....	649
9.15	Smart Defense – Application Intelligence.....	654
9.15.1	General	655
9.15.2	Anti Spoofing Configuration Status.....	656
9.15.3	Network Security	656
9.15.4	Application Intelligence	666
9.15.5	StormCenter	672
9.16	GUIDbedit	675
10 Smart Status und SmartView Tracker		681
11 Authentisierung mit Next Generation.....		715
11.1	Prinzipielles zu den Authentisierungsmethoden	716
11.1.1	Interne Authentisierungsmethoden.....	716
11.1.2	Externe Authentisierungsmethoden	723
11.2	Möglichkeiten zur Benutzerauthentisierung.....	730
11.2.1	User-Authentisierung	730
11.2.2	Client-Authentisierung	737
11.2.3	Session-Authentisierung.....	747
11.2.4	Kombination der Authentisierungsverfahren	752
11.2.5	Reihenfolge der Regeln zur Authentisierung.....	753
11.2.6	Hinweise zur Einrichtung	753
11.3	Einsatz von LDAP-Servern.....	758
11.3.1	LDAP – Lightweight Directory Access Protocol	758
11.3.2	Vorbereitungen bei Next Generation	762
11.3.3	Einrichtung und Verwaltung von Benutzern auf LDAP-Servern.....	762
11.3.4	Nutzung der Authentisierungsmöglichkeit in einer Regelbasis	774
12 Network Address Translation		777
12.1	Notwendigkeit und Möglichkeiten.....	777
12.1.1	RFC 1918	778
12.1.2	Prinzip der NAT.....	781
12.2	Static NAT (Static Mode)	781
12.2.1	Static Destination Mode.....	782
12.2.2	Static Source Mode	783
12.3	Dynamic NAT (Hide Mode)	784
12.4	Möglichkeiten zur Einrichtung der NAT bei Next Generation.....	787
12.4.1	Das NAT-GUI	788

12.4.2	Automatische NAT	789
12.4.3	Manuelle NAT	792
12.5	Mögliche Probleme bei NAT	797
12.5.1	ARP	797
12.5.2	Routing	801
12.5.3	Host-Routing	803
12.5.4	Anti-Spoofing	805
12.5.5	Umgehung vieler Probleme durch globale Einstellungen von NG	806
12.5.6	Mögliche Probleme mit einzelnen Protokollen	807
13	<i>Virtual Private Networks mit NG.....</i>	809
13.1	Verschlüsselung in Next Generation.....	810
13.1.1	Intranet VPN	811
13.1.2	Remote-Access VPN	812
13.1.3	Extranet VPN.....	812
13.1.4	Vollständiges VPN.....	813
13.2	Server-Server VPN (Intranet und Extranet) mit IKE	814
13.2.1	IPSec	814
13.2.2	ISAKMP/OAKLEY und IKE.....	819
13.3	Client-Server VPN mit SecuRemote und SecureClient	826
13.3.1	Das Prinzip von SecuRemote.....	826
13.3.2	Installation von SecuRemote auf einem PC	829
13.3.3	Einrichtung der VPN-1 für die Nutzung von SecuRemote	832
13.3.4	Einrichtung von SecuRemote und der laufende Betrieb	834
13.3.5	Der Einsatz des SecureClient	837
13.3.6	SecureClient in der Praxis.....	845
13.3.7	Das SecureClient Diagnostics Tool	848
13.3.8	Weitere Hinweise zur Konfiguration.....	849
14	<i>Ausfallsicherheit mit Next Generation</i>	861
14.1	Überlappende Verschlüsselungsdomains	862
14.2	Ausfallsicherheit durch Multiple Entry Points (MEP).....	865
14.3	Hochverfügbarkeit für Firewalls	872
14.4	Ausfallsicherheit für das Management	880
15	<i>Die Kommandozeile</i>	885
15.1	Basiskommandos	886
15.2	Allgemeines zu den Kommandos fw, fwm und vpn.....	894
15.3	Kommandos für die Verwaltung von NG	895
15.3.1	Verwaltung der Installation mit cpconfig und cp_conf	895
15.3.2	Lizenzverwaltung	899
15.3.3	Produktverwaltung in SmartUpdate.....	906
15.3.4	Sicherheit beim Bootvorgang	913
15.3.5	Alarmierung	915
15.3.6	Verwaltung und Installation von Regelsätzen	919
15.3.7	Benutzerverwaltung	929
15.3.8	Verwaltung der Logs	940

15.3.9	Kommandos für die Daemons.....	945
15.4	Verwaltung von VPN	947
15.5	Befehle für die Hochverfügbarkeit.....	955
15.6	Wichtige Kommandos beim Upgrade und Wechsel	958
15.7	Kommandos für das Debugging und Monitoring	961
15.7.1	Kontrolle registrierter IP-Adressen bei limitierten Versionen.....	962
15.7.2	Kontrolle der installierten Versionsnummer	962
15.7.3	Das Kommando cpstat.....	963
15.7.4	Überwachung des Datenflusses.....	964
15.7.5	Debugging für fw und fwm	967
15.7.6	Debugging für vpn.....	969
15.7.7	Kontrolle des Kernel-Moduls	971
15.7.8	Kontrolle der State Tables	974
15.8	Sonstiges	975
15.9	Beispiel: Installation einer Regelbasis von Hand.....	976
15.10	Die Sprache INSPECT	977

16 Praktische Konfigurationsbeispiele..... 979

16.1	Hinweise zur Vergabe von Namen	979
16.2	Administratoren- und CPMI-Gruppen einrichten.....	982
16.2.1	Deklaration von Administratoren und -Gruppen.....	982
16.2.2	Deklaration von CPMI-Gruppen	983
16.2.3	Rechte zur Installation von Regeln auf Objekten	984
16.3	Aufbau einer einfachen Regelbasis	984
16.3.1	Reihenfolge der Regeln	985
16.3.2	Anpassung der Grundeinstellungen von NG	987
16.3.3	Spezielle Regeln.....	989
16.4	Nutzung von Ressourcen	993
16.4.1	Ressourcen für SMTP	995
16.4.2	Ressourcen für FTP	998
16.4.3	Ressourcen für HTTP.....	999
16.4.4	Definition eigener Ressourcen.....	1001
16.5	Einbindung und Konfiguration von Alarmen	1003
16.6	Authentisierung von Benutzern für verschiedene Dienste.....	1005
16.6.1	Eingabe von Regeln zur Authentisierung	1005
16.6.2	User-Authentisierung für Telnet und HTTP	1007
16.6.3	User-Authentisierung für FTP.....	1008
16.6.4	Client-Authentisierung	1009
16.6.5	Session-Authentisierung.....	1013
16.7	Remote Management bei Next Generation	1014
16.7.1	Abheben der SmartConsole.....	1014
16.7.2	Trennung von Inspektions- und Management-Modul	1015
16.7.3	Weitere notwendige Zugriffe.....	1017
16.8	Einrichtung von Static NAT und Dynamic NAT.....	1019
16.8.1	Static NAT	1019
16.8.2	Dynamic NAT.....	1021
16.8.3	Weitere Möglichkeiten der NAT.....	1022

16.9	Routerverwaltung mit NG	1024
16.9.1	Grundvoraussetzungen, Regeln und deren Installation.....	1024
16.9.2	Import der ACLs von einem Router.....	1027
16.10	Aufbau fester VPN	1029
16.10.1	Klassisches VPN mit IKE	1030
16.10.2	Vereinfachte Einrichtung eines VPN mit Communities	1036
16.10.3	Aufbau eines Extranets.....	1039
16.11	VPN von Client zu Server	1042
16.11.1	Konfiguration eines Clientless VPN	1042
16.11.2	Sichere Datenübertragung mit SecuRemote	1045
16.11.3	Einsatz von SecureClient und Policy Server	1046
16.12	Load Balancing	1049
16.12.1	Load-Balancing für HTTP	1050
16.12.2	Load-Balancing für FTP und andere Dienste.....	1051
16.12.3	Weiteres zum Load Agent.....	1052
 Anhang: Quellen und Ports		1053
 Stichwortverzeichnis		1061