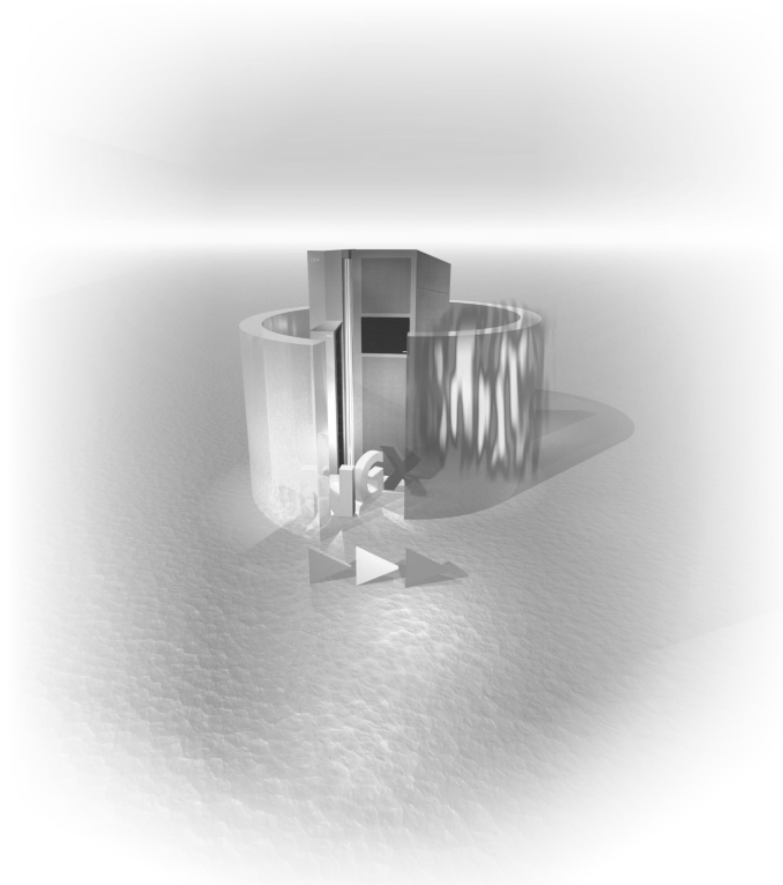




Computer & Literatur Verlag GmbH

CHECK POINT NGX

**Dr. Matthias Leu
und Bernd Ochsmann**



Deutsche Nationalbibliothek – CIP-Einheitsaufnahme
Bibliografische Information der Deutschen Nationalbibliothek

Ein Titeldatensatz für diese Publikation ist bei
der Deutschen Nationalbibliothek erhältlich und im Internet über
<http://dnb.ddb.de> abrufbar.

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des
Herausgebers ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form
durch Fotokopie, Mikrofilm oder ein anderes Verfahren zu vervielfältigen
oder zu verbreiten. Dasselbe gilt für das Recht der öffentlichen Wiedergabe.

Der Verlag macht darauf aufmerksam, daß die genannten Firmen- und
Markenzeichen sowie Produktbezeichnungen in der Regel marken-, patent-,
oder warenzeichenrechtlichem Schutz unterliegen.

Die Herausgeber übernehmen keine Gewähr für die Funktions-
fähigkeit beschriebener Verfahren, Programme oder Schaltungen.

1. Auflage 2007

© 2007 by C&L Computer und Literaturverlag
Zavelsteiner Straße 20, 71034 Böblingen
E-Mail: info@cul.de
WWW: <http://www.CuL.de>

Coverdesign: Hawa & Nöh, Neu-Eichenberg
Satz: C&L-Verlag
Druck: PUT i RB DROGOWIEC
Printed in Poland

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt

ISBN 978-3-936546-37-8

INHALT

1 Vorwort	15
2 Grundlagen von TCP/IP	17
2.1 Die Schichtenmodelle	18
2.2 Netzwerkschicht	20
2.3 Internetschicht.....	21
2.4 Transportschicht	45
2.5 Weitere Protokolle des IP.....	52
2.6 Applikationsschicht.....	55
3 Warum eine Firewall?	59
3.1 Die Offenheit der Protokolle im Internet.....	60
3.2 Schutz durch Firewalls und DMZ	65
3.3 Heutige Anforderungen an Firewalls.....	66
3.4 Absicherung von Applikationen	66
3.5 Ganzheitlicher Ansatz und zentrales Management.....	67
4 Technische Sicherheitsmechanismen	73
4.1 Paketfilter	74
4.2 Circuit Level und Application Level Gateways.....	84
4.3 Stateful Inspection.....	88
4.4 Der heutige Trend	92
5 Grundlagen von NGX.....	95
5.1 Funktionsprinzip von NGX	95
5.2 Secure Virtual Networking und Secure Internal Communication	98
5.3 Die Basiskomponenten von NGX.....	100
5.3.1 Enforcement Point – die Firewall.....	102
5.3.2 SmartCenter – das zentrale Management	104
5.3.3 SmartConsole – das GUI.....	105
5.3.4 SmartPortal – das Webinterface	114

5.4 Optionen von NGX	115
5.4.1 Remote-Management	115
5.4.2 Benutzer-Authentisierung.....	120
5.4.3 Virtual Private Networks	121
5.4.4 Check Point Integrity, InterSpect, Connectra und Edge verwalten.....	123
5.4.5 Ausfallsicherheit und Load Sharing	125
5.4.6 Ausfallsicherheit für die Verwaltung	126
5.4.7 Load Balancing für Server	126
5.4.8 Routerverwaltung mit dem Open Security Manager.....	127
5.4.9 Integration weiterer Software.....	128
5.5 Grundausstattung und Zubehör	130
6 NGX installieren und lizenzieren.....	135
6.1 Installationsplattformen und -anforderungen	136
6.2 Absicherung des Betriebssystems.....	137
6.2.1 Microsoft Windows Server 2003	138
6.2.2 SUN Solaris	142
6.2.3 Red Hat Enterprise Linux	153
6.3 Weitere Betriebssysteme	161
6.3.1 SecurePlatform und SecurePlatform Pro.....	161
6.3.2 Nokia IPSO.....	170
6.4 Inhalte der Installations-CD bei NGX R62.....	173
6.5 NGX unter Windows Server installieren.....	173
6.6 NGX unter Unix installieren	191
6.7 NGX de-installieren	198
6.8 Migration von Version NG AI zu NGX.....	201
6.9 Lizenzierung und Lizenzverwaltung	212
7 SmartDashboard und Grundeinstellungen	237
7.1 Objektbaum, Regelsätze und SmartMap.....	238
7.2 Das Menü und die Werkzeugleiste	240
7.3 Die Grundeinstellungen von NGX.....	266
7.3.1 Allgemeines	266
7.3.2 FireWall.....	266
7.3.3 NAT – Network Address Translation	284
7.3.4 Authentication	288
7.3.5 VPN.....	289
7.3.6 VPN-1 UTM Edge/Embedded Gateway.....	296
7.3.7 Remote Access	297
7.3.8 SmartDirectory (LDAP)	322
7.3.9 QoS	325
7.3.10 SmartMap.....	327
7.3.11 UserAuthority	328

7.3.12 Management High Availability	330
7.3.13 ConnectControl	332
7.3.14 OSE – Open Security Extension	333
7.3.15 Stateful Inspection	335
7.3.16 Log and Alert.....	339
7.3.17 Reporting Tools.....	346
7.3.18 OPSEC.....	348
7.3.19 SmartCenter Access.....	349
7.3.20 Non Unique IP Address Ranges.....	351
7.3.21 SmartDashboard Customization.....	351
7.4 Überprüfung und Installation einer Regelbasis.....	355

8 Objekte in NGX verwalten..... 357

8.1 Allgemeines	358
8.2 Netzwerkobjekte	359
8.2.1 Check Point	363
8.2.2 Nodes.....	370
8.2.3 Interoperable Device	372
8.2.4 Eigenschaften von Check Point, Nodes und Interoperable Device	372
General.....	372
Cluster Members	376
ClusterXL	380
3rd Party Configuration.....	383
Topology	385
ISP Redundancy.....	401
NAT	403
SmartDefense.....	407
VPN	409
Remote Access	419
Authentication	426
SmartDirectory (LDAP)	429
SmartView Monitor	430
UserAuthority Server.....	431
UserAuthority WebAccess	433
Logs and Masters	435
Reporting Tools	442
Capacity Optimization	442
Web Server	444
Mail Server	447
DNS Server	448
Advanced	450
8.2.5 Eigenschaften von Embedded Devices, InterSpect und Connectra	465
8.2.6 Check Point VSX.....	475
8.2.7 Network	477
8.2.8 Domain.....	481
8.2.9 OSE Device	483
8.2.10 Group.....	494

8.2.11 Logical Server	499
8.2.12 Address Ranges.....	505
8.2.13 Dynamic Object	507
8.2.14 VoIP Domains	508
8.3 Services	513
8.3.1 TCP	514
8.3.2 Compound TCP	518
8.3.3 Citrix TCP	518
8.3.4 UDP	519
8.3.5 RPC.....	522
8.3.6 ICMP.....	523
8.3.7 DCE-RPC	524
8.3.8 Other	525
8.3.9 Group	527
8.4 Resources	529
8.4.1 URI.....	531
8.4.2 URI for QoS	547
8.4.3 SMTP.....	548
8.4.4 FTP.....	560
8.4.5 TCP.....	564
8.4.6 CIFS	565
8.5 Servers and OPSEC-Applications	567
8.5.1 RADIUS und Gruppe von RADIUS-Servern.....	568
8.5.2 TACACS	571
8.5.3 LDAP Account Unit.....	572
8.5.4 Certificate Authority.....	581
8.5.5 SecuRemote DNS	585
8.5.6 OPSEC Applications	586
8.6 Users and Administrators.....	600
8.6.1 Allgemeines	602
8.6.2 Administrator Groups – Gruppen von Administratoren	602
8.6.3 Administrators.....	604
8.6.4 External User Profiles	610
8.6.5 LDAP Groups – Benutzergruppen auf LDAP-Servern	614
8.6.6 Templates – Vorlagen für Benutzer.....	615
8.6.7 User Groups – Benutzergruppen.....	616
8.6.8 Users.....	618
8.7 Permission Profiles – Berechtigungsprofile für Administratoren	631
8.7.1 General.....	632
8.7.2 Permissions.....	633
8.8 Time – Zeiten und Zeitpunkte.....	636
8.8.1 Time.....	637
8.8.2 Group	639
8.8.3 Scheduled Event.....	640

8.9 VPN Communities – Grundlage für VPN	641
8.9.1 Site-to-Site.....	642
8.9.2 Remote Access.....	663
8.10 Remote Access – Connection Profile	666
8.11 QoS – Quality of Service Classes	670
8.11.1 DiffServ Class of Service.....	671
8.11.2 Low Latency Class of Service.....	672
8.11.3 DiffServ Class of Service Group	672
8.12 SmartView Monitor – Virtual Links	673
8.13 UserAuthority	676
8.13.1 UA Authentication Domains.....	677
8.13.2 Operations.....	679
8.13.3 Trusts	680
9 Regeln eingeben	683
9.1 Allgemeines	684
9.2 Name der Regel	688
9.3 Bestimmung von Absender und Ziel	689
9.4 Die Spalte VPN	690
9.5 Auswahl an Services oder Ressourcen	692
9.6 Time – Zeitliche Beschränkung	694
9.7 Action – Geforderte Aktionen	695
9.7.1 Accept.....	696
9.7.2 Drop.....	697
9.7.3 Reject.....	698
9.7.4 User Auth	699
9.7.5 Client Auth	699
9.7.6 Session Auth	700
9.8 Track – Die Reaktion der Firewall	700
9.9 Install On – Installationsmöglichkeiten	703
9.10 Comment – das Kommentarfeld	707
9.11 Wichtige Regeln	707
9.11.1 Default-Regel	708
9.11.2 Stealth-Regel	708
9.11.3 Clean-up-Regel	709
9.12 Reihenfolge, in der die Regeln greifen	710
9.13 Reihenfolge der Aktivitäten am Gateway	714
9.14 Regeln verstecken	716
9.15 (Temporäres) Ausschalten von Regeln	716
9.16 Anfragen an die Regelbasis mit Queries	717
9.17 GUIdbedit und dbedit	722

10 Smart Defense, Web Intelligence und Content Inspection.727

10.1 General – Download Updates	729
10.2 Network Security	732
10.2.1 Anti Spoofing Configuration Status	732
10.2.2 Denial of Service	732
10.2.3 IP and ICMP	733
10.2.4 TCP	736
10.2.5 Fingerprint Scrambling	738
10.2.6 Successive Events.....	740
10.2.7 DShield Storm Center	741
10.2.8 Port Scan	745
10.2.9 Dynamic Ports	746
10.3 Application Intelligence.....	747
10.3.1 Mail	748
10.3.2 FTP.....	752
10.3.3 Microsoft Networks.....	753
10.3.4 Peer to Peer	755
10.3.5 Instant Messengers	757
10.3.6 DNS.....	758
10.3.7 VoIP	759
10.3.8 SNMP.....	761
10.3.9 VPN Protocols	762
10.3.10 CA BrightStor Backup	763
10.3.11 Content Protection	763
10.3.12 DHCP.....	763
10.3.13 Socks.....	764
10.3.14 Remote Control Applications	764
10.3.15 Routing Protocols.....	766
10.3.16 MS-RPC	766
10.3.17 SUN-RPC	768
10.3.18 Telnet	768
10.3.19 Veritas Backup Exec Protections	768
10.3.20 MS-SQL.....	769
10.4 Web Intelligence.....	770
10.4.1 General.....	772
10.4.2 Web Servers View.....	773
10.4.3 Malicious Code.....	774
10.4.4 Application Layer	775
10.4.5 Information Disclosure.....	779
10.4.6 HTTP Protocol Inspection	780
10.4.7 HTTP Client Protection.....	785
10.5 Neu seit NGX R62: Profile und Installationsorte	786
10.6 Content Inspection.....	788
10.7 SmartDefense Services.....	797

11 SmartView Tracker und SmartView Monitor	799
11.1 Der SmartView Tracker – Der Blick in das Log	800
11.1.1 Allgemeine Einstellungen und Hinweise	801
11.1.2 Die Werkzeugleiste und Menüs	806
11.1.3 Logeinträge	810
11.1.4 Log: Das klassische Log.....	818
11.1.5 Audit: Log der administrativen Tätigkeiten.....	820
11.1.6 Active: Log der momentan aktiven Verbindungen	823
11.1.7 Sperren aktiver Verbindungen: Block-Intruder	824
11.2 SmartView Monitor – Komponenten überwachen.....	828
11.2.1 Allgemeine Einstellungen und Hinweise	829
11.2.2 Werkzeugleiste und Menüs	831
11.2.3 Gateway Status.....	835
11.2.4 Traffic	839
11.2.5 System Counters	841
11.2.6 Tunnels	842
11.2.7 Remote Users	844
12 Authentisierung mit NGX	845
12.1 Prinzipielles zu den Authentisierungsmethoden	846
12.2 Möglichkeiten der Benutzerauthentisierung	857
12.2.1 User-Authentisierung	857
12.2.2 Client-Authentisierung	864
12.2.3 Session-Authentisierung.....	873
12.2.4 Vergleich der Authentisierungsverfahren	879
12.2.5 Reihenfolge der Regeln zur Authentisierung.....	880
12.2.6 Hinweise zum Einrichten der Authentisierung.....	880
12.3 LDAP-Server	886
12.3.1 LDAP – Lightweight Directory Access Protocol	886
12.3.2 Vorbereitungen bei NGX	889
12.3.3 Benutzer einrichten und verwalten auf LDAP-Servern.....	890
12.3.4 Nutzung der Authentisierung in einer Regelbasis	903
13 Network Address Translation	905
13.1 Notwendigkeit und Möglichkeiten.....	905
13.2 Static NAT (Static Mode)	910
13.3 Dynamic NAT (Hide Mode)	913
13.4 Konfiguration der NAT	916
13.5 Problemzonen der NAT.....	927
13.5.1 NAT auf das externe Interface der Firewall.....	927
13.5.2 ARP.....	928
13.5.3 Routing	933
13.5.4 Host-Routing.....	935

13.5.5 Anti-Spoofing.....	937
13.5.6 Globale Einstellungen von NGX	938
13.5.7 Mögliche Probleme mit einzelnen Protokollen.....	939
13.5.8 NAT und die Kontrollverbindungen von NGX.....	940
13.6 IP-Pool NAT	941
14 Bandbreitenmanagement mit FloodGate-1	943
14.1 Grundsätzliches zu Bandbreitenmanagement.....	943
14.2 Inbetriebnahme von FloodGate-1	945
14.3 Regeln für FloodGate-1.....	947
14.4 Differentiated Services – DiffServ.....	954
14.5 Low Latency Queuing – LLQ	956
14.6 Weitere Optionen von FloodGate-1	958
15 Virtual Private Networks mit NGX	961
15.1 Möglichkeiten in NGX.....	962
15.2 Server-Server VPN mit IKE.....	965
15.2.1 IPsec.....	966
15.2.2 ISAKMP/OAKLEY und IKE.....	971
15.2.3 Domain-Based VPN.....	977
15.2.4 Überlappende VPN-Domains	979
15.2.5 Route-Based VPN – VPN Tunnel Interfaces (VTI).....	983
15.2.6 Weiteres zu dynamischen Routing	999
15.3 Client-Server-VPN mit SecuRemote und SecureClient	999
15.3.1 Das Prinzip von SecuRemote	1000
15.3.2 Installation von SecuRemote auf einem PC	1002
15.3.3 VPN-1 für SecuRemote einrichten	1005
15.3.4 Einrichten von SecuRemote und der laufende Betrieb	1006
15.3.5 SecureClient	1009
15.3.6 SecureClient in der Praxis.....	1022
15.3.7 Das SecureClient Diagnostics Tool.....	1029
15.3.8 Konfiguration von SecuRemote und SecureClient	1031
15.3.9 Das SecureClient Packaging Tool	1042
15.3.10 Übersicht zu Integrity Clients und Integrity SecureClient	1044
15.4 Clientless VPN	1046
15.4.1 Nutzung von SSL für VPN	1046
15.4.2 Der SSL Network Extender.....	1048
15.4.3 Weitere Funktionalität mit Check Point Connectra	1052

16 Ausfallsicherheit	1055
16.1 Ausfallsicherheit für den SmartCenter	1055
16.1.1 Hochverfügbarkeit des Managements.....	1056
16.1.2 Primary und Secondary SmartCenter konfigurieren.....	1056
16.1.3 Arbeiten mit der Management-HA.....	1057
16.2 Hochverfügbarkeit für Firewalls	1060
16.2.1 Prinzipielles zu Check Point ClusterXL	1061
16.2.2 Synchronisierung der State Tables	1064
16.2.3 HA – Ausfallsicherheit mit ClusterXL.....	1065
16.2.4 LS – Load Sharing mit ClusterXL.....	1067
16.2.5 Abschließendes zu ClusterXL	1070
16.2.6 Weitere Optionen für die Konfiguration von Clustern.....	1073
16.3 Ausfallsicherheit für VPN	1074
16.3.1 Multiple Entry Point – Redundanz und Lastverteilung für VPN	1074
16.3.2 Der Route Injection Mechanism (RIM).....	1079
16.3.3 Der Wire Mode.....	1082
16.4 Ausfallsicherheit für Provider: ISP Redundancy	1085
17 Praktische Konfigurationsbeispiele	1093
17.1 Vergabe von Namen	1093
17.2 Administratoren- und CPMI-Gruppen einrichten	1096
17.2.1 Deklaration von Administratoren und -Gruppen	1097
17.2.2 Deklaration von CPMI-Gruppen	1098
17.2.3 Rechte zur Installation von Regeln auf Objekten	1099
17.3 Aufbau einer einfachen Regelbasis	1099
17.3.1 Reihenfolge der Regeln	1100
17.3.2 Grundeinstellungen von NGX anpassen	1102
17.3.3 Implizite Regeln	1103
17.3.4 Spezielle Regeln.....	1108
17.4 Nutzung von Ressourcen	1114
17.4.1 Ressourcen für SMTP	1116
17.4.2 Ressourcen für FTP	1120
17.4.3 Ressourcen für HTTP.....	1121
17.4.4 Definition eigener Ressourcen	1122
17.5 Einbindung und Konfiguration von Alarmen.....	1124
17.6 Einrichtung von Static NAT und Dynamic NAT	1127
17.6.1 Static NAT	1127
17.6.2 Dynamic NAT	1130
17.6.3 Weitere Möglichkeiten der NAT.....	1131
17.7 ConnectControl	1132
17.7.1 Load-Balancing für HTTP	1133
17.7.2 Load-Balancing für FTP und andere Dienste.....	1134
17.7.3 Weiteres zum Load Agent	1135

17.8 Routerverwaltung mit NGX	1135
17.8.1 Grundvoraussetzungen, Regeln und deren Installation	1136
17.8.2 Import der ACLs von einem Router.....	1139
17.9 Authentisierung von Benutzern für verschiedene Dienste .	1141
17.9.1 Eingabe von Regeln zur Authentisierung.....	1141
17.9.2 User-Authentisierung für Telnet und HTTP.....	1143
17.9.3 User-Authentisierung für FTP	1144
17.9.4 Client-Authentisierung	1145
17.9.5 Session-Authentisierung	1150
17.10 Clientless VPN	1151
17.10.1 Konfiguration von NGX für Clientless VPN.....	1152
17.10.2 Der SSL Network Extender.....	1154
17.11 VPN-Clients	1156
17.11.1 Sichere Datenübertragung mit SecuRemote	1156
17.11.2 SecureClient und Policy Server.....	1158
17.11.3 Der Integrity SecureClient.....	1164
17.12 Aufbau fester VPN im Simplified Mode	1165
17.12.1 Basiskonfiguration fester VPN.....	1165
17.12.2 Vermaschtes VPN	1166
17.12.3 Sternförmiges VPN	1168
17.12.4 Authentisierung über ein Pre-Shared Secret	1169
17.12.5 Authentisierung durch Zertifikate	1170
17.12.6 Hinweise auf einige mögliche Konfigurationsfehler	1172
17.13 VPN-Routing.....	1173
 Anhang A:	
Die Kommandozeile.....	1179
A.1 Basisbefehle.....	1181
A.2 Die Befehle fw, fwm und vpn.....	1183
A.3 NGX verwalten.....	1185
A.4 VPN verwalten	1230
A.5 Hochverfügbarkeit.....	1237
A.6 Upgrade und Wechsel	1239
A.7 Debugging und Monitoring.....	1241
A.8 Wichtige Dateien im Supportfall: cpinfo	1257
A.9 Sonstiges.....	1260
A.10 Beispiel: Regelbasis von Hand installieren.....	1261
A.11 Die Sprache INSPECT.....	1263
 Anhang B:	
Weiterführendes	1265
Stichwortverzeichnis.....	1273

KAPITEL 1:

VORWORT

Dieses Buch behandelt Check Point NGX, eine Firewall, die schon wieder einen neuen Namen bekommen hat. Sie ist die Weiterentwicklung der bereits legendären und seit über zehn Jahren erhältlichen FireWall-1 beziehungsweise VPN-1 von Check Point. In diesem Buch geht es um die Version NGX R62, falls notwendig, werden Hinweise auf die vorhergehenden Versionen von NGX gegeben.

Speziell die Öffnung von Netzwerken nach außen sowie zum Internet erfordern Schutzmechanismen, damit Fremde nicht auf die vertraulichen Daten eines Unternehmens zugreifen können. Die Kopplung von Netzwerken zwischen Unternehmen, die in bestimmten Bereichen zusammenarbeiten, ist normal. Nicht immer herrscht aber zwischen den Unternehmen ein uneingeschränktes Vertrauen, weshalb Sicherheitsmaßnahmen ergriffen werden müssen. aber auch dann, wenn das Unternehmen seine IT-Struktur an das Internet angebunden hat.

Viele der heute gewünschten Maßnahmen sind über Router und andere Geräte umsetzbar. Check Point NGX bietet als Sicherheitslösung diese und noch viel mehr Möglichkeiten. Es handelt sich dabei um eine reine Softwarelösung, die auf das Betriebssystem einer Maschine aufsetzt. Mindestens jede vierte Sicherheitslösung, die weltweit installiert wird, ist eine von Check Point. Wenn die Sicherheitspolitik des Unternehmens dies vorsieht, kann NGX das richtige Werkzeug zur Absicherung des Unternehmensnetzwerkes sein, sie ist es aber nicht zwangsläufig in jedem Fall. Auch andere Firewalls haben ihre Vorteile, so daß NGX auf keinen Fall grundsätzlich und immer als die einzige und optimale Lösung angesehen werden darf! Beispielsweise kann das Sicherheitskonzept des Unternehmens fordern, daß die Sicherheitslösung auf einem proprietären und damit auch Angreifern unbekanntem Betriebssystem aufsetzen muß. Dann ist NGX, die auf verschiedenen Standard-Betriebssystemen läuft, nicht immer das Mittel der Wahl.

Das Arbeitsprinzip der Check Point FireWall-1/VPN-1 bietet viele Vorteile, fordert aber eine sehr gute Ausbildung des Administrators und ein hohes Maß an Verantwortungsbewußtsein. Dieses Buch hilft diesen Fachleuten, NGX genauer kennenzulernen und zu verstehen.

Danksagung

An diesem Buch haben uns viele Freunde, Kollegen und Mitarbeiter geholfen, denen wir an dieser Stelle herzlich danken möchten. Vor allem aber danken beide Autoren ihren Familien sehr herzlich für die Geduld und die Zeit, die das Schreiben dieses Buches erforderte, von den Nerven ganz zu schweigen. Besonderer Dank gilt Rubina Leu, die nun schon zum dritten Mal ein Buch über die FireWall-1 »ertragen« hat. Gegenüber den vorigen Büchern zu diesem Thema war diesmal die Zeit, die sie Matthias entbehren mußte, besonders hoch. Trotzdem hatte sie immer Verständnis und Geduld – herzlichen Dank!

Unermüdlich gearbeitet haben auch viele andere, die einzelne Passagen oder auch das ganze Manuskript vor Ihnen gelesen und vor allem viele Korrekturen und Verbesserungsvorschläge eingebracht haben. Stellvertretend für viele möchten wir hier speziell Dr. Peter Bieringer, Robert Binder, Fritz Eberhart, Harald Geiger, Thomas Greschitz, Timo Jobst, Viktor Mraz und dem Team von Check Point Deutschland danken. Ihre vielen Tips und hilfreichen Hinweise haben dieses Buch erst zu dem werden lassen, was es unter dem Strich geworden ist.

München, am Beginn des Jahres 2007
Dr. Matthias Leu und Bernd Ochsmann

Über die Autoren

Dr. Matthias Leu stammt aus Hamburg, das er 1980 verließ, um in München zu studieren. Heute arbeitet der diplomierte Physiker und promovierte Ingenieur der Elektrotechnik als geschäftsführender Gesellschafter der AERAssec Network Services and Security GmbH in Hohenbrunn bei München. Seit 1995 hat er unzählige FireWall-1 beziehungsweise VPN-1 installiert, auditiert und im Bereich Troubleshooting »repariert«.

Das vorliegende, seiner Frau Rubina gewidmete Buch, ist bereits sein drittes zur Check Point FireWall-1/VPN-1.

Bernd Ochsmann stammt aus Bockenem nahe Hildesheim und studierte Physik an der Universität Hannover. Bereits 1991 sammelte der diplomierte Physiker erste Linux- und Internet-Erfahrungen. Seit Juni 2000 ist er direkt beim Hersteller der VPN-1, Check Point Software, angestellt und arbeitet dort im Bereich Professional Services und Second Level Support direkt für das israelische Headquarter. Er leitet und erarbeitet Projekte für die größten Unternehmen weltweit und hat bereits mehrere bekannte Whitepaper für Check Point Software geschrieben. Seine Spezialgebiete sind neben der VPN-1 die High End Produkte Provider-1, VSX und GX für Mobilfunknetze.

Für Kommentare, Anfragen und Kritik zu diesem Buch per E-Mail an mleu@aerasesc.de und bochsman@checkpoint.com sind die Autoren immer offen und freuen sich auf Ihre Rückmeldung. Vielen Dank.