Yasushi Kono

Check Point VPN-1 Power

Das umfassende Handbuch

Galileo Press

Inhalt

Geleitwort des Fachgutachters 21
Vorwort 23
Über das Buch 25

1 Allgemeines zu Internet-Security und Firewalls 41

1.1 Die Firewall-Technologien im Überblick 42
1.1.1 Der Paketfilter 44
1.1.2 Das Application Layer Gateway 45
1.1.3 Das Circuit Level Gateway 45
1.1.4 Die Stateful Inspection 46
1.2 Internet Security ist mehr! 53
1.2.1 IPSec VPN 54
1.2.2 Public Key Infrastructure 54
1.2.3 SSH 56
1.2.4 SSL/TLS 57
1.3 Zusammenfassung 58

2 Die grundlegende Architektur der Check Point-Firewall 61

2.1 Secure Internal Communication (SIC) 62
2.1.1 Was ist SIC, und wozu wird sie benötigt? 62
2.1.2 Wie funktioniert SIC? 63
2.2 Check Points dreischichtige Architektur 63
2.3 Die Architektur der Check Point VPN-1-Software 65
2.3.1 Das Modul CPRID 66
2.3.2 Die Befehle zum Starten und Stoppen der Module und CPShared 67
2.3.3 Das Reinitialisieren des Firewall-Moduls FW1 68
2.3.4 Das Reinitialisieren des VPN-Moduls 68
2.3.5 Das Neustarten des CPHA-Moduls 68
2.3.6 Beenden und Starten von SmartPortal 69
2.3.7 Beenden und Starten von QoS 69
2.3.8 Starten und Beenden des Advanced Routing-Moduls 70
2.4 Interne Mechanismen bei cprestart 70
2.5 Zusammenfassung 71

3 Installation von Check Point VPN-1 Power 73

3.1 Ein Wort zur Lizenzierung von Check Point-Produkten 74
3.1.1 Verwaltung von Lizenzen 75
3.1.2 Einige Informationen zu den SKU-Features 79
3.2 Die unterstützten Betriebssysteme von Check Point NG und NGX 80
3.3 Hardware-Voraussetzung für Check Point NG/NGX 81
3.3.1 Die Appliances der NOKIA IP-Serie 83
3.4 Installation unter Windows 87
3.4.1 Härten von Windows 87
3.4.2 Installation des Check Point Security Gateways in einem Distributed Deployment 89
3.4.3 Installation des Check Point SmartCenters in einem Distributed Deployment 98
3.4.4 Standalone Installation 107
3.5 Installation unter Solaris 112
3.5.1 Installationstipp für Solaris 9 112
3.5.2 Installationstipp für Solaris 10 117
3.5.3 Installation von Check Point VPN-1 Pro/Power auf Solaris 117
3.6 Installation unter SecurePlatform 119
3.6.1 Installation des Check Point Security Gateways in einem Distributed Deployment (Konfiguration per Kommandozeile) 120
3.6.2 Installation des Check Point Security Gateways in einem Distributed Deployment (Konfiguration per Web) 126
3.6.3 Installation des SmartCenters in einem Distributed Deployment 135
3.6.4 Standalone Installation unter SecurePlatform 138
3.7 Installation unter IPSO 140
3.8 Default Policy 149
3.9 Zusammenfassung 150

4 Besondere Merkmale der Betriebssysteme 153

4.1 SecurePlatform und SecurePlatform Pro 153
4.1.1 Standard Mode 154
4.1.2 Der Expert Mode 162
4.1.3 Weitere Expert Mode-Befehle 165

4.1.4 Erweiterte Expert Mode-Features ... 168
4.1.5 Zugriff über die WebUI ... 170
4.1.6 Webzugriff über HTTPS auf SecurePlatform ... 171
4.2 Nokia IPSO ... 172
4.3 Sun Solaris unter SPARC ... 184
4.3.1 Booten von CD-ROM ... 185
4.3.2 Mounten einer CD ... 185
4.3.3 IP Forwarding (Packet Forwarding, Routing) ... 185
4.3.4 Deinstallation von Check Point unter Solaris ... 186
4.4 Windows 2000 Server/ Windows Server 2003 ... 186
4.4.1 IP Forwarding ... 187
4.4.2 Deinstallation der Check Point Software unter Windows ... 188
4.5 Zusammenfassung ... 188

5 SmartConsole Tools und SmartPortal ... 193

5.1 Was ist SMART? ... 193
5.1.1 SmartDashboard ... 193
5.1.2 Die Elemente von SmartDashboard ... 198
5.1.3 Elemente neben dem Object Tree ... 207
5.1.4 SmartView Tracker ... 217
5.1.5 SmartView Monitor ... 225
5.1.6 SmartLSM ... 228
5.1.7 Eventia Reporter ... 229
5.1.8 SmartUpdate ... 239
5.1.9 SmartPortal ... 243
5.2 Zusammenfassung ... 248

6 Elementare Regeln und Implied Rules ... 251

6.1 Notwendige Vorbereitungen ... 252
6.1.1 Die Anti-Spoofing-Konfiguration der Security Gateways ... 254
6.1.2 Multicast-Beschränkung bei den Security Gateways ... 255
6.2 Erstellen eines Fremd-Firewall-Objekts ... 256
6.3 Erstellen von sonstigen Host-Objekten ... 258
6.4 Erstellen von Netzwerk-Objekten ... 259
6.5 Das Erstellen von Benutzer-Objekten ... 261
6.6 Die Stealth Rule ... 262
6.7 Die Cleanup Rule ... 264

6.8 Services unter Check Point ... 264
6.9 Regel für den FTP-Zugriff ... 267
6.10 Regel für den ausgehenden HTTP-Zugriff ... 269
6.11 Implied Rules ... 273
6.12 Control Connections ... 275
6.13 Wann wird eine Regel wirksam? ... 286
6.14 Was passiert, wenn SIC wegbricht? ... 287
6.15 Remote Firewall und SmartCenter Server mit privater IP-Adresse ... 289
6.16 Zusammenfassung ... 290

7 Migration von NG nach NGX ... 291

7.1 Allgemeines zur Migration ... 291
7.2 Bevor Sie anfangen ... 292
7.3 Die möglichen Migrationsmethoden ... 292
7.4 Migration der SmartCenter Server von FP3/R54/R55 nach R6x ... 293
7.4.1 SmartCenter-Upgrade von SecurePlatform R55 auf R6x (Distributed Deployment) ... 293
7.4.2 SmartCenter-Upgrade mittels »Upgrade Tools« ... 302
7.4.3 SmartCenter Upgrade von SecurePlatform FP3 auf NGX ... 305
7.4.4 SmartCenter Upgrade unter Windows 2000/2003 von R60 auf R6x > R60 ... 306
7.4.5 SmartCenter Upgrade unter Nokia IPSO von R55 auf R60 ... 311
7.4.6 Upgrade des Check Point NG SmartCenter nach NGX ... 314
7.4.7 Management High Availability Upgrade unter SecurePlatform R55 nach R60 ... 316
7.5 Migration von R54/R55 Security Gateways nach R6x ... 318
7.5.1 Firewall-Upgrade von SecurePlatform R54/R55 auf R60 mit SmartUpdate ... 318
7.5.2 Firewall-Upgrade von SecurePlatform R54/R55 auf R60 mit »patch add«-Kommandos ... 322
7.5.3 Cluster-Upgrade von Nokia-VRRP-Cluster von R60 auf R61 ... 322
7.5.4 Migration von Nokia IP Clustering von R60 nach R61 ... 329
7.6 Post-Upgrade Tasks ... 331
7.7 Provider-1 Upgrade ... 332
7.7.1 MDG-Installation unter Windows ... 333
7.7.2 Inplace Upgrade auf SecurePlatform ... 333

7.8 Upgrade eines Provider-1 CMAs auf NGX MDS 336
7.9 Zusammenfassung 340

8 Authentication unter Check Point 343

8.1 Client Authentication unter Check Point VPN-1 Pro NGX 345
8.1.1 Sign On Method: »Manual« 347
8.1.2 Sign On Method: »Partially Automatic« 350
8.1.3 Sign On Method: »Fully Automatic« 351
8.1.4 Sign On Method: »Agent Automatic Sign On« 351
8.1.5 Sign On Method: »Single Sign On« 351
8.2 User Authentication unter Check Point VPN-1 Pro NGX 353
8.3 Session Authentication unter Check Point VPN-1 Pro/Power NGX 359
8.4 Integration von SecurID 362
8.5 Authentifizierung mittels RADIUS Server (Beispielkonfiguration unter MS Internet Access Service) 369
8.6 Authentifizierung mit TACACS bzw. TACACS+ 375
8.7 Zusammenfassung 376

9 LDAP-Integration 381

9.1 Allgemeines zur LDAP-Integration 381
9.2 Was ist LDAP? 382
9.3 Was ist eine LDAP-Integration? 385
9.4 LDAP-Integration: MS Active Directory 385
9.4.1 Modifikation des bestehenden Active Directory-Schemas 389
9.4.2 Kommunikation über LDAP-SSL 399
9.5 LDAP-Integration: Novell NDS/eDirectory 403
9.6 LDAP-Integration: Sun ONE Directory Server 5.2 412
9.7 Zusammenfassung 419

10 Network Address Translation 421

10.1 Hide NAT (Dynamic NAT) 423
10.1.1 Konfiguration von Hide NAT mittels Automatic NAT 425
10.1.2 Hide NAT via Manual NAT 426
10.1.3 Allgemeine Anmerkung zu Hide NAT 427

10.2 Static NAT 427
10.2.1 Allow Bi-Directional NAT 428
10.2.2 Translate Destination on Client Side 430
10.2.3 Automatic ARP Configuration 435
10.2.4 Konfiguration von Static NAT 437
10.3 Manual NAT 438
10.4 IP Pool NAT 441
10.5 Zusammenfassung 445

11 VPN unter Check Point 447

11.1 Phase 1: Aufbau einer IKE SA (Internet Key Exchange Security Association) im Main Mode 449
11.2 Der Diffie-Hellman-Algorithmus 450
11.3 Phase 1: Aufbau einer IKE SA im Aggressive Mode 452
11.4 Phase 2: Aufbau einer IPSec SA 454
11.5 Site-to-Site VPN (Domain Based) zwischen zwei Check Point Gateways 456
11.5.1 Site-to-Site VPN zwischen zwei Check Point Security Gateways mit gemeinsamem SmartCenter Server 456
11.5.2 Site-to-Site VPN zwischen zwei Check Point Security Gateways mit jeweils eigenem SmartCenter 458
11.5.3 Advanced Settings 462
11.5.4 VPN Star Community 464
11.5.5 Syntax von »vpn_route.conf« 466
11.5.6 Advanced Settings bei VPN Star Community 469
11.6 Traditional Mode versus Simplified Mode 470
11.7 Directional VPN bei Site-to-Site VPN 474
11.7.1 Einschränkungen von Directional VPN 474
11.7.2 Konfiguration von Directional VPN 475
11.8 Site-to-Site VPN (Route Based) 475
11.8.1 Konfiguration von VTIs 477
11.8.2 Konfiguration von dynamischem Routing 479
11.9 Site-to-Site VPN zwischen Check Point VPN-1 Pro/Power und VPN-1 Edge Appliance 483
11.10 Site-to-Site VPN zwischen einem Check Point Gateway und einem anderen Gateway 486
11.10.1 Was müssen Sie nun bei der Konfiguration beachten? ... 489
11.10.2 Phase 1 (IKE SA bzw. ISAKMP SA): 489
11.10.3 Phase 2 (IPSec SA): 490
11.10.4 Reinitialisierung eines bestehenden VPN-Tunnels 492

11.10.5 Exkurs: Cisco und OSE 493
11.11 Remote Access VPN 497
11.11.1 SecuRemote 497
11.11.2 Definition einer VPN Site 505
11.11.3 Authentifizierung über Certificate 507
11.11.4 Die Client-Information in der Datei userc.C 510
11.11.5 Das SecureClient Packaging Tool 515
11.11.6 SecureClient 526
11.11.7 Grundlegende Konfiguration von Regeln für Remote Access VPN mit SecureClient 532
11.11.8 SecureClient und Office Mode 534
11.11.9 SecureClient und Hub Mode 539
11.11.10 Konvertierung von Traditional Mode in Simplified Mode 545
11.11.11 Steuerung des SecureClient per CLI 547
11.11.12 Directional VPN bei Remote Access VPN 549
11.11.13 Remote Access VPN mit der VPN-1 Edge X-Appliance 550
11.12 Zusammenfassung 552

12 Hochverfügbarkeitslösungen 555

12.1 Allgemeines zu Hochverfügbarkeitslösungen 555
12.2 Management HA (High Availability) 558
12.3 ClusterXL 566
12.3.1 Installation von ClusterXL auf Security Gateways unter MS Windows 2000/2003 567
12.3.2 Installation von ClusterXL auf Security Gateways unter SecurePlatform 568
12.3.3 Konfiguration von ClusterXL 569
12.4 Lösungen unter Nokia: VRRP Monitored Circuit und IP Clustering 575
12.4.1 Installation auf Nokia IPSO: VRRP Monitored Circuit 575
12.4.2 Installation auf Nokia IPSO: IP Clustering 585
12.5 Multiple Entry Point 592
12.5.1 Die Konfiguration von Multiple Entry Point 593
12.5.2 Das Problem des asymmetrischen Routings 594
12.5.3 Bestimmung der verfügbaren Routen mit Hilfe von RIM 596
12.5.4 MEP in Verbindung mit Remote Access VPN 598
12.6 ConnectControl 599

12.7 Hochverfügbarkeit von VPN-1 Edge 603
12.8 Hochverfügbarkeit bei Provider-1 604
12.8.1 Installation eines Secondary MDS Managers 605
12.8.2 Hochverfügbarkeit einzelner CMAs 610
12.9 Zusammenfassung 613

13 SmartDefense 617

13.1 Die neue Registerkarte »SmartDefense Services« 618
13.1.1 Download Updates 619
13.1.2 Advisories 619
13.1.3 Security Best Practices 619
13.2 Die übrige Aufteilung von SmartDefense 620
13.2.1 Download Updates 620
13.2.2 Protection Overview 620
13.2.3 Network Security 621
13.2.4 Application Intelligence 628
13.2.5 Web Intelligence 633
13.3 Ein mögliches Szenario 638
13.4 SYN Flood & LAND Attack 640
13.5 Zusammenfassung 642

14 Analyse-Tools 645

14.1 WireShark 646
14.2 Monitoring von Paketen mit »fw monitor« 647
14.2.1 Syntaktische Beispiele für einfache fw monitor-Kommandos 648
14.2.2 Weitere Filterausdrücke 659
14.3 Monitoring von SecureClient-Paketen 660
14.4 Tcpdump 661
14.5 CPInfo 663
14.5.1 Erstellen einer CPInfo-Output-Datei 664
14.5.2 Analyse der CPinfo-Output-Datei 665
14.6 Die fw tab-Kommandos 666
14.7 Lizenz-Analyse mit LicViewer 670
14.8 IKEView für die Analyse von IKE/IPsec 671
14.9 Das Kommando fw ctl pstat 672
14.10 Dimensionierung des Kernel-Speichers 676
14.11 Debugging mit »fw ctl debug« 677
14.12 Debugging von SecureClient 679

14.13 Die Daemons »fwd« und »fwm« in den Debug Mode versetzen ... 681
14.14 Zusammenfassung ... 682

15 Verwaltungstools für die Objekt-datenbank ... 685

15.1 Änderung einiger Parameter in den Global Properties ... 686
15.1.1 Network Address Translation ... 688
15.1.2 Management High Availability ... 689
15.2 Erstellen von Host-Objekten mit dbedit ... 689
15.3 Erstellen von Service-Objekten mit dbedit ... 690
15.4 Beispiele weiterer Modifikationen mit dbedit ... 691
15.4.1 Excessive Log Grace Period ... 691
15.4.2 Modifikation der SA-Lifetimes für IKE und IPSec ... 692
15.4.3 Konfiguration von Mail Alert ... 692
15.4.4 Anlegen eines Benutzer-Objekts ... 693
15.4.5 Optimieren von Gateway-Eigenschaften ... 693
15.5 Die grafische Entsprechung zu dbedit: GUIdbedit ... 696
15.6 Zusammenfassung ... 700

16 Voice over IP: Konfiguration unter Check Point NGX ... 701

16.1 Die wesentlichen Merkmale von VoIP ... 702
16.2 H.323 ... 706
16.2.1 H.323 Terminal ... 707
16.2.2 H.323 Gatekeeper ... 707
16.2.3 H.323 Gateway ... 707
16.2.4 Multipoint Control Unit (MCU) ... 707
16.3 Session Initiation Protocol (SIP) ... 711
16.3.1 Die Komponenten von SIP ... 711
16.3.2 Die SIP Response Codes ... 713
16.3.3 Verlauf einer SIP-Kommunikation ... 715
16.4 Vergleich: SIP gegen H.323 ... 716
16.5 Konfiguration von Asterisk als SIP Proxy ... 717
16.5.1 /etc/asterisk/sip.conf ... 718
16.5.2 /etc/asterisk/extensions.conf ... 719
16.5.3 /etc/asterisk/voicemail.conf ... 719
16.6 Installation und Konfiguration von OnDO SIP Server als SIP Proxy ... 720
16.7 Basiskonfiguration von SIP User Agents ... 723
16.7.1 Konfiguration von GrandStream BudgeTone 100 ... 724

16.7.2 Konfiguration von Allnet ALL7950 728
16.7.3 Softphones 731
16.8 Konfiguration von Check Point für SIP-Kommunikation 733
16.9 Konfiguration von Check Point für H.323-Kommunikation 735
16.10 Zusammenfassung 737

17 Quality of Service 741

17.1 Die QoS-Technologien 742
17.2 Die QoS Policy von Check Point 743
17.2.1 Express Mode 744
17.2.2 Traditional Mode 745
17.3 Der Einsatz von QoS Classes 747
17.3.1 Konfiguration der Gateway-Interfaces 749
17.4 Zusammenfassung 755

18 Troubleshooting VPN-1 Pro/Power 759

18.1 Probleme mit SIC 759
18.2 Probleme mit der Policy Installation 762
18.2.1 Installation wird mit Fehlern abgebrochen 762
18.2.2 Probleme nach einem Wechsel von DAIP zu einer Firewall mit statischer IP 763
18.2.3 Probleme nach dem Erstellen von zwei Host-Objekten mit gleicher IP-Adresse 764
18.2.4 Error: macro identifier <fw> redefined. Compilation failed. 765
18.2.5 [LOG-CRIT] kernel: FW-1: Log Buffer is full 765
18.2.6 [LOG-CRIT] kernel: FW-1: lost 500 log/trap messages ... 766
18.2.7 Error: No valid QoS license 766
18.2.8 Firewall-HQ-01 NGX R62 QoS. Verifier Error in Standard. DiffServ Class DSCP1010 is not defined for this interface. 766
18.2.9 Policy installation failed 766
18.2.10 Classes guarantees must not exceed interface rate 767
18.3 Probleme mit der CheckPoint-Installation 768
18.3.1 InError:CPshrd/cpshared_ipso.tgz depend on /opt/CPshared-50-04 768
18.3.2 Probleme bei Solaris 9: libCrun.so.1: open failed: No such file or directory 768

18.3.3 Probleme mit der HFA-Installation auf Nokia Flash-based Appliances ... 769
18.3.4 Das Hinzufügen von externem Zusatzspeicher in einer Flash-based Nokia IP Appliance schlägt fehl ... 770
18.4 Probleme mit einer URI-Ressource ... 771
18.5 Probleme mit der Konfiguration von ClusterXL ... 773
18.6 Probleme mit der SIP-Kommunikation ... 774
18.7 Probleme mit Site-to-Site VPN ... 775
18.8 Probleme mit Remote-Access-VPN ... 781
18.9 Probleme mit der LDAP-Integration ... 781
18.10 Probleme mit Upgrade-Tools ... 782
18.11 Probleme mit der Installation von Provider-1 R55 ... 783
18.12 Probleme nach dem Inplace-Upgrade von Provider-1 NGX R60A nach NGX R62 ... 783
18.13 QoS-Probleme ... 784
18.14 Fehlermeldung von SmartDefense ... 784
18.15 Fehlerhaftes Verhalten bei ClusterXL unter SecurePlatform ... 785
18.16 Die Policy lässt sich nicht von einem SmartCenter Server auf die VPN-1 Edge X-Appliance installieren ... 785
18.17 Zusammenfassung ... 787

19 Backup und Restore ... 789

19.1 Backup und Restore unter Windows ... 791
19.1.1 Security Gateway ... 791
19.1.2 SmartCenter Server ... 792
19.2 Backup und Restore unter SecurePlatform ... 795
19.2.1 Backup und Restore des Security Gateways ... 796
19.2.2 Backup und Restore des SmartCenter Servers ... 806
19.2.3 Upgrade-Tools unter SecurePlatform ... 807
19.3 Sicherung und Wiederherstellung unter IPSO ... 810
19.3.1 Backup and Restore ... 810
19.3.2 Configuration Sets ... 813
19.4 Zusammenfassung ... 815

20 Neuerungen von NGX R65 ... 819

20.1 Systemvoraussetzungen für VPN-1 Power/ UTM NGX R65 ... 819
20.1.1 Benötigte Betriebssysteme ... 820
20.1.2 Mindestvoraussetzungen für den NGX SecureClient ... 820
20.1.3 Hardware-Mindestvoraussetzungen ... 820

20.2 Upgrade auf R65 821
20.2.1 SmartCenter Upgrade unter Windows 823
20.2.2 SmartCenter Upgrade unter Linux, SecurePlatform und Solaris 824
20.2.3 SmartCenter Upgrade unter Nokia IPSO 825
20.2.4 Offline-Migration des SmartCenters nach R65 825
20.3 Bootvorgang unter SecurePlatform/SecurePlatform Pro 826
20.4 Installation des SmartCenters auf SecurePlatform 827
20.5 Installation des SmartCenters unter Windows 828
20.6 Web Filtering und Anti Virus unter R65 829
20.7 Interface Bonding 833
20.8 Die Advisories im SmartView Tracker 833
20.9 SecurePlatform- und Linux-Unterstützung für Intel Active Management Technology 834
20.10 SmartDefense und Aggressive Aging 834
20.11 Service und Aggressive Aging 835
20.12 SYN Cookie 836
20.13 Management Plug-ins 837
20.14 Zusammenfassung 837

Anhang 839

A RSA SecurID 841
A.1 Grundsätzliches zu RSA Authentication Manager 6.1 841
A.1.1 Die Tokens von RSA SecurID 842
A.1.2 Installation unter Windows 2000 Server bzw. Advanced Server 845
A.1.3 Installation des RSA Authentication Agents auf dem Server 850
A.1.4 Installation unter Red Hat Enterprise Linux 3 861
A.2 Zur Erinnerung: Integration von SecurID in die Check Point SVN 866
A.3 Zusammenfassung 867
B Administration der VPN-1 Edge Appliances mit dem SmartCenter Server NGX R62 871
B.1 Die Modelle und Features der VPN-1 Edge-Serie 871
B.2 Initiale Konfiguration der VPN-1 Edge 872
B.3 Integration der VPN-1 Edge Appliances in die Smart-Infrastruktur 873

B.4 Aktualisieren der VPN-1 Edge Firmware von Embedded NG auf Embedded NGX ... 883
B.5 Zusammenfassung ... 886
C Administration von SofaWare Safe@Office Appliances über SofaWare SMP ... 889
C.1 Safe@Office Appliances ... 889
C.2 Initiale Konfiguration der Safe@Office-Appliance ... 890
C.3 Was kann die Safe@Office-Appliance? ... 893
C.3.1 Welcome ... 894
C.3.2 Reports ... 895
C.3.3 Security ... 897
C.3.4 Services ... 903
C.3.5 Network ... 903
C.3.6 Setup ... 909
C.3.7 VPN ... 916
C.3.8 Help ... 918
C.3.9 Logout ... 919
C.4 Die SMP-Architektur ... 919
C.5 SofaWare Management Server (SMS) ... 920
C.5.1 Event Logging Module ... 920
C.5.2 URL Filtering Module (UFM) ... 920
C.5.3 Content Vectoring Module (CVM) ... 921
C.5.4 Dynamic VPN Service (DVPN) ... 921
C.5.5 Dynamic DNS Service (DDNS) ... 921
C.5.6 SofaWare Reporting Module ... 921
C.6 SofaWare Management Center (SMC) ... 922
C.7 Self Provisioning Portal (SPP) ... 922
C.8 Installation von SMP ... 922
C.8.1 Voraussetzung für die Installation ... 922
C.8.2 Installation des Primary SMP Servers unter Windows ... 923
C.9 Am SMC anmelden ... 931
C.10 Konfiguration des SMP ... 932
C.11 Erstellen eines Service-Plans vom Typ »Local Management« ... 935
C.12 Erstellen eines Service-Plans vom Typ »Remote Management« ... 938
C.13 Erstellen eines Gateways ... 940
C.14 Registrierung des Gateways an dem SMS ... 942
C.15 Firmware-Update ... 945
C.16 Noch einmal: Registrierung der Appliance an den SMS ... 950
C.17 Zusammenfassung ... 952

D Check Point Provider-1 957
D.1 Wozu dient Provider-1? 957
D.1.1 Network Operation Center (NOC) 958
D.1.2 Multi Domain Server & CMAs 958
D.1.3 MSP 959
D.1.4 MDG 959
D.1.5 CLM 959
D.2 Installation von Provider-1 960
D.2.1 Die unterstützten Betriebssysteme 960
D.2.2 Hardware-Mindestvoraussetzung 960
D.2.3 Installationsschritte 961
D.3 Installation der Multi Domain GUI 964
D.3.1 Die unterstützten Betriebssysteme und die Hardware-Mindestanforderungen 964
D.3.2 Installation der MDG unter Windows 965
D.3.3 Installation der MDG unter Solaris 965
D.4 Konfiguration von CMAs 966
D.4.1 Anlegen eines neuen Customers 966
D.4.2 Modifizieren von administrativen Zugriffsrechten 968
D.5 Wichtige Kommandozeilenbefehle zu Provider-1 971
D.6 Verwaltung der Logs 977
D.7 Die Global Policies 982
D.8 Umwandeln eines SmartCenter Servers in einen Customer 984
D.9 Sicherung Ihres MDS-Systems 986
D.10 Wiederherstellung Ihres MDS-Systems 987
D.11 Praxisszenario 989
D.12 Zusammenfassung 991
E Check Point Integrity 995
E.1 Die Architektur von Integrity 995
E.2 Installation des Integrity Servers 996
E.2.1 Voraussetzung für die Installation 996
E.2.2 Vorgehensweise bei der Installation 997
E.3 Die Entities von Integrity 1001
E.4 Die administrativen Rollen in Integrity 1002
E.5 Die Integrity Clients 1003
E.6 Die Organisation der Zonen 1005
E.7 Die Integrity Security Policies 1006
E.8 Die Policy Rules 1007
E.9 Installation des Integrity Clients 1017

E.10 Wenn die Software einmal installiert ist ... 1019
E.11 Zusammenfassung ... 1020
F Das ISO-/OSI-Referenzmodell ... 1025
F.1 Bitübertragungsschicht ... 1025
F.2 Sicherungsschicht ... 1026
F.3 Vermittlungsschicht ... 1028
F.4 Transportschicht ... 1029
F.5 Sitzungsschicht ... 1030
F.6 Darstellungsschicht ... 1030
F.7 Anwendungsschicht ... 1030
G Literaturhinweise und Tipps ... 1033
G.1 Literatur zu Check Point NG/NGX VPN-1 Pro/Power ... 1033
G.2 Weitere Informationen zum Thema Check Point ... 1034
G.3 Grundlegende Konzepte ... 1035
G.4 Voice over IP ... 1035
G.5 Hacking ... 1035
G.6 OS Fingerprinting ... 1036
G.7 SofaWare SMP ... 1036
G.8 LDAP und X.500 ... 1037
G.9 VMWare ... 1037
H Glossar ... 1039

Index ... 1053