

<b>Preface</b>	<b>Accelerated Check Point Security Administration II NGX (R65)</b>	1
Course Layout		2
Prerequisites		2
Recommended Setup for Labs		3
Recommended Lab Topology		4
IP Addresses		5
Lab Terms		7
Check Point Security Architecture		8
Unified Security Architecture		9
Complete Protection		10
Broad Range of Security Solutions		11
Network Security		12
Data Security		14
Security Management		15
Services		16
Training and Certification		17
CCMA		18
Learn More		18
<b>Chapter 1</b>	<b>Installing and Upgrading VPN-1</b>	19
Preinstallation Configuration		21
Distributed Installation		23
Upgrading to VPN-1 NGX R65		24
Upgrade Guidelines		24
Upgrade Order		25
Upgrade Export/Import		25
Upgrading via SmartUpdate		26
VPN-1 Backward Compatibility		27
Supported Versions		27
Licensing VPN-1		29
Obtaining Licenses		29
Supported Upgrade Paths		31
Contract Verification		31
Performing License Upgrade		33
Pre-Upgrade Considerations		35
Pre-Upgrade Verification Tool		35
Web Intelligence License Enforcement		35
Upgrading on SecurePlatform		36
Upgrading SmartCenter Server		37
Using the Pre-Upgrade Verification Tool		37
Gateway Upgrade		40
Gateway Upgrade with SmartUpdate		40
Review		73
Review Questions		73
Review Answers		74

<b>Chapter 2</b>	<b>Introduction to SecurePlatform</b>	75
	Introduction	77
	SecurePlatform Hardware Requirements and Setup	78
	Hardware Compatibility Testing Tool	78
	Using the Command Line	80
	Basic Linux Commands	80
	Backup and Restore	83
	Viewing Scheduling Status in the WebUI	85
	Restoring the Backup via the Command Line	85
	Restoring Older Versions of SecurePlatform	87
	Scheduling a Backup in the WebUI	88
	Viewing the Backup Log in the WebUI	89
	Generating CPIInfo	89
	Critical Check Point Directories	90
	Log Files	90
	objects.C and objects_5_0.C	90
	rulebases_5_0.fws	91
	fwauth.NDB	91
	Exporting User Database Only	91
	Backing Up Using upgrade_export	92
	Managing Your SecurePlatform System	94
	Connecting to SecurePlatform Using Secure Shell	94
	User Management	95
	SecurePlatform Command Shell	96
	SecurePlatform Command Shell	96
	Management Commands	97
	Documentation Commands	98
	System Commands	99
	Snapshot-Image Management	100
	System-Diagnostic Commands	101
	Check Point Commands	102
	Network-Diagnostic Commands	105
	Network-Configuration Commands	106
	User and Administrative Commands	109
	Lab 2: Configuring VPN-1 Using the CLI	111
	Review	121
	Review Questions	121
	Review Answers	122
<b>Chapter 3</b>	<b>SmartUpdate</b>	123
	Introduction to SmartUpdate	125
	SmartUpdate Architecture	126
	Upgrading Packages	128
	Prerequisites for Remote Upgrades	128
	Retrieving Data From VPN-1 Gateways	129
	Adding New Packages to the Package Repository	129
	Verifying the Viability of a Distribution	129
	Transferring Files to Remote Devices	130
	Upgrading Edge Firmware with SmartUpdate	131
	Rebooting the VPN-1 Gateway	131

Recovering From a Failed Upgrade . . . . .	131
Deleting Packages From the Package Repository . . . . .	132
<b>Managing Licenses . . . . .</b>	<b>133</b>
License Upgrade . . . . .	134
Retrieving License Data From VPN-1 Gateways . . . . .	134
CPInfo . . . . .	135
SmartUpdate Command Line . . . . .	136
Lab 3: Creating Objects, Establishing Trust and Configuring SmartMap . . . . .	139
Lab 4: Configuring the Security Policy . . . . .	159
Review . . . . .	171
Review Questions . . . . .	171
Review Answers . . . . .	172
<b>Chapter 4   Monitoring Traffic and Connections . . . . .</b>	<b>173</b>
SmartView Tracker . . . . .	175
SmartView Tracker Login . . . . .	176
Log Types . . . . .	176
SmartView Tracker Tabs . . . . .	178
Action Icons . . . . .	180
Log-File Management . . . . .	181
Administrator Auditing . . . . .	182
Global Logging and Alerting . . . . .	182
Time Settings . . . . .	185
Blocking Connections . . . . .	187
Terminating and Blocking Active Connections . . . . .	187
SmartView Monitor . . . . .	189
SmartView Monitor Login . . . . .	191
Customizable Views . . . . .	191
Monitoring Suspicious Activity Rules . . . . .	198
Monitoring Alerts . . . . .	198
SmartView Tracker vs. SmartView Monitor . . . . .	202
Eventia Reporter . . . . .	204
Report Types . . . . .	206
Predefined Reports . . . . .	208
Customizing Predefined Reports . . . . .	210
Eventia Reporter Considerations . . . . .	211
Eventia Reporter Licensing . . . . .	214
Lab 5: Blocking Intruder Connections . . . . .	215
Lab 6: Configuring Suspicious Activity Rule in SmartView Monitor . . . . .	225
Review . . . . .	237
Review Questions . . . . .	237
Review Answers . . . . .	238
<b>Chapter 5   Basic SmartDefense and Content Inspection . . . . .</b>	<b>239</b>
Introducing SmartDefense . . . . .	241
Networks and Application Intelligence . . . . .	242
Web Intelligence . . . . .	243
Online Updates . . . . .	243

Monitor Only Mode .....	244
Network Security .....	246
Denial-of-Service .....	246
IP and ICMP .....	248
TCP .....	248
Fingerprint Scrambling .....	249
Successive Events .....	250
DShield Storm Center .....	251
Port Scanning .....	253
Application Intelligence .....	256
Mail .....	256
FTP .....	257
Microsoft Networks .....	258
Peer-to-Peer .....	258
Instant Messaging .....	258
DNS .....	259
VoIP .....	260
SNMP .....	260
Web Intelligence .....	262
Web Intelligence Protections .....	262
Web Intelligence License Enforcement .....	264
SmartDefense Services .....	267
Download Updates Tab .....	267
Advisories Tab .....	269
Security Best Practices Tab .....	271
Content Inspection .....	272
Introduction to Integrated Antivirus and Web-Filtering Technologies .....	272
Database Updates .....	273
Antivirus-Scan Settings .....	274
Web Filtering .....	282
Lab 7: Configuring SmartDefense .....	285
Lab 8: Configuring Web-Filtering and Antivirus Settings .....	311
Review .....	327
Review Questions .....	327
Review Answers .....	328

<b>Chapter 6 Site-to-Site VPNs .....</b>	<b>329</b>
Site-to-Site VPN .....	331
Domain-Based VPN .....	331
Route-Based VPN .....	333
VPN Routing Process for VTIs .....	333
Routing Multicast Packets Through VPN Tunnels .....	337
VPN Tunnel Management .....	339
Permanent Tunnels .....	339
VPN Tunnel Sharing .....	343
Wire Mode .....	345
Wire Mode in a MEP Configuration .....	346
Wire Mode with Route-Based VPN .....	347
Wire Mode Between Two VPN Communities .....	348

Directional VPN Enforcement . . . . .	350
Directional Enforcement Between Communities . . . . .	352
Multiple Entry Point VPNs . . . . .	354
VPN High Availability with MEP . . . . .	354
Traditional Mode VPNs . . . . .	355
Lab 9: Two-Gateway IKE Encryption (Shared Secret) . . . . .	359
Review . . . . .	357
Review Questions . . . . .	357
Review Answers . . . . .	358
<b>Chapter 7 Remote Access VPNs . . . . .</b>	<b>383</b>
Remote Access VPN . . . . .	385
Extending SecuRemote with SecureClient . . . . .	386
Connect Mode . . . . .	387
Establishing Remote Access — Workflow . . . . .	388
Office Mode . . . . .	389
How Office Mode Works . . . . .	390
Office Mode Planning . . . . .	392
IP Pool vs. DHCP . . . . .	392
Routing-Table Modifications . . . . .	392
Multiple External Interfaces . . . . .	392
Before Configuring Office Mode . . . . .	393
Desktop Security Policy . . . . .	394
Policy Expiration and Renewal . . . . .	394
Policy Server HA . . . . .	395
Wireless Hotspot/Hotel Registration . . . . .	395
Logging . . . . .	396
SecureClient Mobile . . . . .	396
VPN Routing — Remote Access . . . . .	398
Hub Mode . . . . .	399
SSL Network Extender . . . . .	401
How SSL Network Extender Works . . . . .	402
Prerequisites . . . . .	402
Clientless VPN . . . . .	405
Special Considerations for Clientless VPN . . . . .	408
Configuring Clientless VPN . . . . .	409
Creating Appropriate Rules in the Rule Base . . . . .	409
Lab 10: Configuring Remote Access in an IKE VPN . . . . .	411
Review . . . . .	423
Review Questions . . . . .	423
Review Answers . . . . .	424
<b>Chapter 8 High Availability and ClusterXL . . . . .</b>	<b>425</b>
Management High Availability . . . . .	427
Management High Availability Environment . . . . .	429
Synchronization Status . . . . .	429

ClusterXL .....	432
Load Sharing .....	434
ClusterXL Modes .....	435
Legacy High Availability Mode .....	435
New High Availability Mode .....	436
Load Sharing Multicast Mode .....	438
Load Sharing Unicast (Pivot) Mode .....	438
Cluster Control Protocol .....	441
Synchronizing Clusters .....	443
The Synchronization Network .....	443
How State Synchronization Works .....	444
Synchronized-Cluster Restrictions .....	445
Sticky Connections .....	447
The Sticky Decision Function .....	447
CPHA Commands .....	449
cphastart .....	449
cphastop .....	449
cphaprob .....	449
cphaprob Example .....	451
fw hastat .....	454
Debugging ClusterXL Issues .....	455
fw ctl pstat Sync Output .....	456
ClusterXL Configuration Issues .....	458
Modes of ClusterXL Supporting SecureXL .....	458
Crossover-Cable Support .....	458
Lab 11: Deploying New Mode HA .....	459
Review .....	483
Review Questions .....	483
Review Answers .....	484