

---

# Contents

<b>Course Objectives</b>	xiii
<b>Preface Check Point Security Administrator R70</b>	1
Course Layout	2
Prerequisites	2
Certification Title	2
Sample Setup for Labs	3
Training and Certification	6
CCMA	6
Learn More	6
<b>Chapter 1 Check Point Technology Overview</b>	7
Network Access Control	9
The Check Point Firewall	11
Security Gateway Inspection Architecture	17
Deployment Strategies	20
The DMZ	22
Bridge Mode	23
Security Policy Management	25
SmartConsole Components	25
Security Management Server	37
Basic Concepts and Terminology	37
Managing Users in SmartDashboard	39
Creating Administrators in SmartDashboard	40

---

Securing Channels of Communication .....	43
Administrative Login Using SIC .....	48
Review .....	51
Review Questions .....	51
Review Answers .....	52
<b>Chapter 2   Check Point Software Blades</b> .....	<b>53</b>
Check Point Software Blade Architecture .....	54
Selecting your Software Blade .....	57
Building a Security Solution using Software Blades .....	60
Software Blade Containers .....	62
Choosing a Predefined Turnkey System .....	63
Systems .....	64
Security Gateway R70 .....	75
Open Performance Architecture .....	75
Performance Architecture Evolution .....	77
Review .....	83
Review Questions .....	83
Review Answers .....	84
<b>Chapter 3   Deployment Platforms</b> .....	<b>85</b>
UTM-1 Edge Appliances .....	87
UTM-1 Edge Series .....	87
Power-1 Appliances .....	91
IP Appliance .....	92
Managing the IP Appliance .....	93
IP Network Voyager .....	94
IPSO .....	94
IPSO Routing Daemon (IPSRD) .....	96
IP Clustering in IPSO .....	97
Command Line Interface (CLI) .....	98
Disk Mirroring (RAID Level 1) .....	98
Introduction to Voyager .....	100
IPSO File System and Directory Structure .....	101
The IPSO/config Directory .....	102
IPSO /image Directory .....	103

---

IPSO File System and Partitions . . . . .	104
IPSO File System and Partitions . . . . .	105
Diskless File System. . . . .	105
CLISH — IPSO’s Dedicated Configuration Shell . . . . .	106
Command-Line Movement and Editing . . . . .	108
Command Completion . . . . .	109
Command Recall . . . . .	111
Command Help . . . . .	112
Top Level Commands . . . . .	113
CLISH Script Commands . . . . .	113
IP Network Voyager . . . . .	116
Navigating within Voyager. . . . .	118
Configuration and Monitor Menus . . . . .	119
SecurePlatform . . . . .	120
SecurePlatform Hardware Requirements and Setup . . . . .	121
Hardware Compatibility Testing Tool . . . . .	121
Using the Command Line. . . . .	123
Basic Linux Commands . . . . .	123
Backup and Restore . . . . .	126
Viewing Scheduling Status in the WebUI . . . . .	128
Restoring the Backup via the Command Line . . . . .	128
Restoring Older Versions of SecurePlatform . . . . .	130
Scheduling a Backup in the WebUI. . . . .	131
Viewing the Backup Log in the WebUI. . . . .	132
Generating CPInfo . . . . .	132
Critical Check Point Directories . . . . .	133
Log Files . . . . .	133
objects.C and objects_5_0.C . . . . .	133
rulebases_5_0.fws . . . . .	134
fwauth.NDB. . . . .	134
Exporting User Database Only . . . . .	134
Backing Up Using upgrade_export . . . . .	135
Managing Your SecurePlatform System . . . . .	137
Connecting to SecurePlatform Using Secure Shell. . . . .	137
User Management . . . . .	138
SecurePlatform Command Shell. . . . .	139
SecurePlatform Command Shell . . . . .	139
Management Commands . . . . .	140
Documentation Commands . . . . .	141
System Commands . . . . .	142

---

Snapshot-Image Management . . . . .	143
System-Diagnostic Commands . . . . .	144
Check Point Commands . . . . .	145
Network-Diagnostic Commands . . . . .	148
Network-Configuration Commands . . . . .	149
User and Administrative Commands . . . . .	152
Review . . . . .	153
Review Questions . . . . .	153
Review Answers . . . . .	154

## **Chapter 4 Introduction to the Security Policy** 155

Security Policy Basics . . . . .	158
The Rule Base . . . . .	158
Managing Objects in SmartDashboard . . . . .	159
SmartDashboard and Objects . . . . .	160
Managing Objects . . . . .	162
Changing the View in the Objects Tree . . . . .	164
Creating the Rule Base . . . . .	166
Basic Rule Base Concepts . . . . .	166
Default Rule . . . . .	166
Basic Rules . . . . .	169
Implicit/Explicit Rules . . . . .	170
Control Connections . . . . .	172
Detecting IP Spoofing . . . . .	176
Completing the Rule Base . . . . .	179
Understanding Rule Base Order . . . . .	179
Rule Base Management . . . . .	180
Review . . . . .	180
Useful Tips . . . . .	180
Policy Management and Revision Control . . . . .	182
Policy-Management Overview . . . . .	183
Policy Packages . . . . .	184
Installation Targets . . . . .	186
Querying and Sorting Rules and Objects . . . . .	188
Database Revision Control . . . . .	192
Implementing Database Revision Control . . . . .	192
Network Address Translation . . . . .	195
IP Addressing . . . . .	196

---

Hide NAT	197
Static NAT	199
Choosing the Hide Address in Hide NAT	201
Configuring Automatic NAT	201
Hide NAT Object Configuration	204
Manual NAT	208
Multicasting	212
Configuring Multicast Access Control	212
Review	215
Review Questions	215
Review Answers	216

## **Chapter 5 Monitoring Traffic and Connections** 217

SmartView Tracker	219
SmartView Tracker Login	220
Log Types	220
SmartView Tracker Tabs	222
Action Icons	223
Log-File Management	225
Administrator Auditing	228
Global Logging and Alerting	228
Time Settings	231
Blocking Connections	233
Terminating and Blocking Active Connections	233
SmartView Monitor	235
SmartView Monitor Login	237
Customizable Views	237
Monitoring Suspicious Activity Rules	244
Monitoring Alerts	244
SmartView Tracker vs. SmartView Monitor	249
Eventia Reporter	250
Report Types	252
Predefined Reports	254
Customizing Predefined Reports	256
Eventia Reporter Considerations	257
Eventia Reporter Licensing	260
Review	261
Review Questions	261
Review Answers	262

---

<b>Chapter 6</b>	<b>Using SmartUpdate</b>	263
	SmartUpdate and Managing Licenses . . . . .	265
	Understanding SmartUpdate . . . . .	266
	SmartUpdate Introduction . . . . .	267
	Overview of Managing Licenses . . . . .	269
	License Attachment Process . . . . .	273
	Service Contracts . . . . .	278
	Licensing R70 . . . . .	284
	Obtaining a License Key . . . . .	284
	Software Installation Packages . . . . .	286
	Gateway Upgrade . . . . .	287
	SmartUpdate Options . . . . .	287
	The SmartUpdate Command Line . . . . .	289
	Review . . . . .	291
	Review Questions . . . . .	291
	Review Answers . . . . .	292
<b>Chapter 7</b>	<b>Upgrading to R70</b>	293
	Preinstallation Compatibility . . . . .	295
	Supported Upgrade Paths . . . . .	297
	Backward Compatibility for Gateways . . . . .	297
	IPS-1 Upgrade Paths and Interoperability . . . . .	298
	Important R70 Upgrade Notes . . . . .	298
	Upgrade Configuration . . . . .	300
	Distributed Installation . . . . .	302
	Pre-Upgrade Considerations . . . . .	302
	Upgrading the Security Management Server . . . . .	304
	Gateway Upgrade . . . . .	306
	Upgrading a Clustered Deployment . . . . .	306
	Review . . . . .	307
	Review Questions . . . . .	307
	Review Answers . . . . .	308
<b>Chapter 8</b>	<b>User Management and Authentication</b>	309
	Creating Users and Groups in SmartDashboard . . . . .	311
	User Types . . . . .	311

---

Security Gateway Authentication . . . . .	313
Introduction to Authentication Methods . . . . .	313
Authentication Schemes . . . . .	315
Remote User Authentication . . . . .	317
Authentication Methods . . . . .	319
User Authentication . . . . .	319
Configuring User Authentication . . . . .	325
Session Authentication . . . . .	326
Configuring Session Authentication . . . . .	327
Client Authentication . . . . .	328
Configuring Client Authentication . . . . .	333
Resolving Access Conflicts . . . . .	335
Configuring Authentication Tracking . . . . .	336
LDAP User Management with SmartDirectory . . . . .	337
LDAP Features . . . . .	337
Multiple LDAP Servers . . . . .	339
Using an Existing LDAP Server . . . . .	340
Configuring Entities to Work with the Gateway . . . . .	340
Managing Users . . . . .	346
SmartDirectory Groups . . . . .	347
Review . . . . .	349
Review Questions . . . . .	349
Review Answers . . . . .	350

## **Chapter 9 Encryption and VPNs** 351

Securing Communication . . . . .	353
Privacy . . . . .	353
Symmetric Encryption . . . . .	354
Symmetric Disadvantages . . . . .	355
Asymmetric Encryption . . . . .	356
Diffie-Hellman . . . . .	356
Integrity . . . . .	358
Authentication . . . . .	359
Two Phases of Encryption . . . . .	361
Encryption Algorithms . . . . .	362
IKE . . . . .	363
ISAKMP . . . . .	363
Oakley . . . . .	363
ISAKMP/Oakley . . . . .	363
Phase 1 . . . . .	364

---

Phase 2 . . . . .	365
How a VPN Works. . . . .	366
Tunneling-Mode Encryption. . . . .	369
<b>Certificate Authorities</b> . . . . .	<b>371</b>
Certificates . . . . .	371
Multiple Certificate Authorities . . . . .	372
Local Certificate Authority . . . . .	372
CA Service via the Internet. . . . .	373
Internal Certificate Authority . . . . .	375
Creating Certificates. . . . .	375
<b>Review</b> . . . . .	<b>377</b>
Review Questions. . . . .	377
Review Answers . . . . .	378

## **Chapter 10 Introduction to VPNs** 379

The Check Point VPN. . . . .	381
<b>VPN Deployments</b> . . . . .	<b>383</b>
Site-to-Site VPNs. . . . .	383
Remote-Access VPNs. . . . .	383
<b>VPN Implementation</b> . . . . .	<b>384</b>
Three Critical VPN Components. . . . .	384
VPN Setup . . . . .	385
VPN Communities . . . . .	387
VPN Topologies. . . . .	389
Choosing a Topology . . . . .	391
Authentication Between Community Members . . . . .	395
Domain and Route-Based VPNs . . . . .	396
Access Control and VPN Communities. . . . .	397
Excluded Services . . . . .	400
Special Considerations for Planning a VPN Topology . . . . .	400
Integrating VPNs into a Rule Base . . . . .	401
<b>Simplified vs. Traditional Mode VPNs</b> . . . . .	<b>403</b>
<b>VPN Tunnel Management</b> . . . . .	<b>404</b>
Permanent Tunnels. . . . .	404
VPN Tunnel Sharing . . . . .	407
<b>Remote Access VPNs</b> . . . . .	<b>409</b>
Multiple Remote Access VPN Connectivity Modes. . . . .	410
Establishing a Connection Between a Remote User and a Gateway . . . . .	410

---

Configuring Remote Access VPN . . . . .	413
Review . . . . .	415
Review Questions . . . . .	415
Review Answers . . . . .	416
<b>Chapter 11    Messaging and Content Security</b>	<b>417</b>
Antivirus Protection . . . . .	419
Anti-Virus Signature Database Updates . . . . .	420
Antivirus Scanning . . . . .	422
Content Security Scanning in Practice . . . . .	423
File Type Recognition . . . . .	429
Continuous Download . . . . .	430
Logging and Monitoring . . . . .	431
File Size Limitations and Scanning . . . . .	432
UTM-1 Edge Antivirus . . . . .	433
Basic URL Filtering . . . . .	435
Architecture . . . . .	435
Anti-Spam and Mail . . . . .	437
Anti-Spam . . . . .	437
Architecture . . . . .	439
Logging and Monitoring . . . . .	441
Reporting False Positives to Check Point . . . . .	442
Review . . . . .	445
Review Questions . . . . .	445
Review Answers . . . . .	446
<b>Chapter 12    Check Point IPS</b>	<b>447</b>
IPS Overview . . . . .	449
New IPS Engine/Architecture . . . . .	451
Flexible IPS Policy Management . . . . .	453
IPS Event Manager . . . . .	455
Configuring and Managing IPS . . . . .	456
IPS Protection . . . . .	460
IPS Profiles . . . . .	462
Creating Profiles . . . . .	462
Assigning Profiles . . . . .	464
Protections Browser . . . . .	466

---

Exporting the Protections List . . . . .	468
Protection Parameters . . . . .	468
<b>Activating Protections . . . . .</b>	<b>473</b>
Automatically Activating Protections . . . . .	473
Manually Activating Protections . . . . .	476
<b>Monitoring Traffic . . . . .</b>	<b>477</b>
Network Exceptions . . . . .	478
Viewing Packet Information . . . . .	479
<b>Optimizing IPS . . . . .</b>	<b>482</b>
Performance Management . . . . .	482
Tuning Protections . . . . .	486
IPS Policy Settings . . . . .	486
Enhancing System Performance . . . . .	487
<b>Updating Protections — IPS Subscription . . . . .</b>	<b>489</b>
Managing IPS Subscriptions . . . . .	489
Updating IPS Protections . . . . .	489
Downloading Updates . . . . .	490
<b>Review . . . . .</b>	<b>491</b>
Review Questions . . . . .	491
Review Answers . . . . .	492

<b>Appendix A SecurePlatform Command Shell . . . . .</b>	<b>493</b>
Command-Line Editing Keys . . . . .	493
Management Commands . . . . .	494
Documentation Commands . . . . .	495
System Commands . . . . .	496
System-Diagnostic Commands . . . . .	497
Check Point Commands (included with IPSO and Solaris) . . . . .	498
Network-Diagnostic Commands . . . . .	501
Network-Configuration Commands . . . . .	502
User and Administrative Commands . . . . .	505

---

## **Appendix B Integrated Content Security with OPSEC Applications**

	507
Security Servers . . . . .	508
Deploying OPSEC Servers . . . . .	510
URL Security Management Applications . . . . .	514
TCP Security Server . . . . .	518
Configuring Content Security . . . . .	519
Creating and Using a Resource . . . . .	520
Antivirus Checking for Incoming Email . . . . .	520
Configuring CVP for Web Traffic Performance . . . . .	523
Configuring URL Filtering - UFP Server . . . . .	524
CVP/UFP Inspection on any TCP Service . . . . .	528

