

Table of Contents

Preface Check Point Security Expert R70	1
Course Layout	2
Prerequisites	2
Certification Title	2
Sample Setup for Labs	3
Training and Certification	10
CCMA	10
Learn More	10
Chapter 1 Management Portal	11
Web Based Administration	12
Deploying the Management Portal - Dedicated Server	12
Deploying the Management Portal - Security Management Server	13
Management Portal Commands and Configuration	13
Client Side Requirements	14
Review	17
Review Questions	17
Review Answers	18
Chapter 2 SmartWorkflow	19
Change Management	20
The SmartWorkflow Environment	20
Task Flow	21
SmartWorkflow Toolbar	24
The SmartWorkflow Session Management Window	25
SmartWorkflow Session Information	28
Working with SmartWorkflow	30
Assigning Permissions	30
Enabling SmartWorkflow	31
Configuring SmartWorkflow	31
Working with Sessions	33

Comparing Policies	37
Approving Sessions	39
Auditing Changes	41
Review	43
Review Questions	43
Review Answers	44

Chapter 3 SmartProvisioning 45

SmartProvisioning Overview	46
SmartProvisioning Management	47
Supported Platforms	48
Enabling SmartProvisioning	49
SmartProvisioning Console	52
Tree Pane	52
Workspace Pane	53
Status View	55
SmartProvisioning Wizard	57
SmartProvisioning Profiles	59
Security Gateway-Only SmartProvisioning	61
Gateway Management	63
Adding Gateways to SmartProvisioning	63
Gateway Edit Windows	63
Real-Time Gateway Actions	67
Remotely Controlling Gateways	67
Editing Gateway Properties	69
Configuring Interfaces	69
Executing Commands	70
Managing SmartLSM Security Gateways	71
Applying Dynamic Object Values	71
Getting Updated Security Policy	72
Changing Assigned SmartLSM Security Profile	72
Tracking	73
Log Servers	74
Configuring SmartLSM Gateway Topology	75
Managing Security Gateways	77
Scheduling Backups	77
Configuring Hosts	78
Configuring the Domain	78

Configuring Host Name	79
Configuring Routing.	79
Managing Software	80
The Package Repository	80
Distributing Packages	82
Security Gateway Actions.	82
Applying Changes	85
Maintenance Mode.	85
UTM-1 Edge Portal	88
UTM-1 Edge Ports	88
Provisional Settings	89
Understanding Dynamic Objects	92
Benefits of Dynamic Objects	92
Dynamic Object Types	92
Dynamic Object Values	93
Command Line.	94
Review.	97
Review Questions.	97
Review Answers	98

Chapter 4 SSL Portal-Based VPN 99

Connectra Unified Secure Remote Access Gateway	100
Key Features	100
Deploying Connectra	102
Deploying Connectra - DMZ	102
Deploying Connectra - LAN	103
Deploying Connectra - Cluster	104
Connectra Requirements	106
Hardware	106
Hardware Compatibility Testing Tool	107
Installation and Configuration Workflow.	109
Installation and Configuration Stages	109
Firewall Access Rules	110
Connecting to the Admin User Interface	112
Logging-In for the First Time	113
Defining Connectra Objects (Central Management)	113
Connecting a Cluster	114
Configuring Access Control	114
Defining Applications.	114

SmartDefense Update	115
Check Your Setup	115
Cluster Deployment	116
Cluster Interfaces	116
Physical Connectivity	117
Configuration	117
Administration	117
SSL Acceleration Card	117
Review	119
Review Questions	119
Review Answers	120
Chapter 5 Acceleration	121
Acceleration	122
SecureXL: Security Acceleration	122
CoreXL: Multicore Acceleration	133
Supported Platforms and Features	133
Default Configuration	134
Performance Tuning	135
Allocating Processing Cores	136
Allocating a Core for Heavy Logging	137
Review	139
Review Questions	139
Review Answers	140
Chapter 6 High Availability	141
Management High Availability	142
The Management High Availability Environment	143
Active vs. Standby	144
Synchronization Modes	145
Synchronization Status	146
Review	149
Review Questions	149
Review Answers	150

Chapter 7	Clustering	151
	ClusterXL: Smart Load Balancing	152
	Installing ClusterXL	154
	Cluster Control Protocol	160
	Cluster Synchronization	161
	Check Point State Synchronization	161
	Synchronized-Cluster Restrictions	162
	Sticky Connections	164
	The Sticky Decision Function	164
	ClusterXL Configuration Issues	166
	Modes of ClusterXL Supporting SecureXL	166
	Crossover-Cable Support	166
	VRRP Overview	167
	How VRRP Works	168
	Review	173
	Review Questions	173
	Review Answers	174
Chapter 8	Advanced Networking - Routing	175
	Advanced Networking Blade	176
	Preferences in Routing	176
	Check Point Dynamic Routing	178
	The Command Line Interface	181
	User Execution Mode	181
	Privileged Execution Mode	181
	Global Configuration Mode	182
	Router Configuration Mode	182
	Interface Configuration Mode	183
	Interfaces	183
	Kernel Interface	183
	Martian Addresses	185
	Multicast Commands	186
	Trace Options	186
	Border Gateway Protocol (BGP)	187
	Internet Control Message Protocol (ICMP)	191
	Open Shortest Path First	191
	Redirect Processing	194

Router Discovery	195
SNMP Multiplexing (SMUX).....	197
Distance Vector Multicast Routing Protocol (DVMRP)	198
Internet Group Management Protocol (IGMP).....	199
Protocol Independent Multicast.....	199
Access Lists	201
AS Paths and AS Path Lists	201
BGP Communities and Community Lists	203
Prefix Lists and Prefix Trees	203
Route Aggregation and Generation	204
Route Flap Damping.....	204
Route Maps	205
Multicast Access Control	206
Multicast Routing Protocols	206
Dynamic Registration Using IGMP.....	206
IP Multicast Group Addressing.....	207
Reserved Local Addresses	207
Review.....	211
Review Questions.....	211
Review Answers	212

Chapter 9 Advanced Networking - Load Balancing	213
Load Balancing	214
Connect Control.....	214
Methods of Load-Balancing	215
ConnectControl Packet Flow	216
Logical Server Types	216
Persistent Server Mode.....	220
Server Availability	222
Load Measuring	222
Review.....	225
Review Questions.....	225
Review Answers	226

Chapter 10	Advanced Networking - QoS	227
	Quality of Service	228
	QoS Technology - Stateful Inspection	229
	QoS Architecture	232
	QoS Gateway	232
	QoS Security Management Server	233
	QoS SmartConsole	233
	QoS Configuration	235
	QoS Policy Management	238
	Bandwidth Allocation and Rules	241
	Default Rule	242
	QoS Action Properties	243
	Example of a Rule Matching VPN Traffic	244
	Bandwidth Allocation and Sub-Rules	245
	Implementing the Rule Base	246
	Deploying QoS	247
	Sample Bandwidth Allocations	249
	Review	253
	Review Questions	253
	Review Answers	254

Chapter 11	Reporting	255
	Introduction to Reporter	256
	Log Consolidation	258
	Predefined Reports	260
	Standard Reports	260
	Express Reports	260
	Report Subjects	261
	Planning for Eventia Reporter	265
	Standalone vs. Distributed Deployment	265
	Log Availability vs. Log Storage and Processing	265
	Record Availability vs. Database Size	266
	High Availability	266
	Adapting Report Detail Level to Needs	266
	Generating Only Selected Sections	267
	Scheduling Reports	267
	Report Filters	267
	Report Output	268

Reporter Database Management	271
Tuning the Database	271
Modifying the Database	271
Predefined Consolidation Policy	272
Review	275
Review Questions	275
Review Answers	276

Chapter 12 IPS Event Analysis 277

Introduction to IPS Event Analysis	278
IPS Event Analysis Architecture	279
IPS Event Analysis Client	282
Initial Configuration	284
The IPS Event Analysis GUI Client	286
Analyzing Events	288
Reports	290
Timeline	290
Graphs	292
Managing Events	295
Events	295
Events	297
Event Viewing	298
Permission Profiles	299
Investigating Events	301
Tracking Events with Tickets	301
Analyzing Events	301
Displaying Log Entries	302
Custom Commands	302
Configuring Event Policy	303
Dynamic Updates	304
Review	307
Review Questions	307
Review Answers	308