
Contents

Course Objectives	xiii
--------------------------------	------

Preface: Check Point Security Administration II NGX (R65)	1
Course Layout	2
Prerequisites	2
Check Point Certified Security Expert (CCSE)	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
Check Point Training and Certification	17
Check Point Certified Master Architect (CCMA)	18
Learn More	18

Chapter 1	SmartUpdate	19
	Introduction to SmartUpdate	21
	SmartUpdate Architecture	22
	Upgrading Packages	24
	Prerequisites for Remote Upgrades	24
	Retrieving Data From VPN-1 Gateways	25
	Adding New Packages to the Package Repository	25
	Verifying the Viability of a Distribution	25
	Transferring Files to Remote Devices	26
	Upgrading Edge Firmware with SmartUpdate	27
	Rebooting the VPN-1 Gateway	27
	Recovering From a Failed Upgrade	27
	Deleting Packages From the Package Repository	28
	Managing Licenses	29
	License Upgrade	30
	Retrieving License Data From VPN-1 Gateways	30
	CPInfo	31
	SmartUpdate Command Line	32
	Lab 1: Updating an Installation with SmartUpdate	35
	Review	49
	Review Questions	49
	Review Answers	50
Chapter 2	Upgrading VPN-1	51
	Preinstallation Configuration	53
	Distributed Installation	55
	Upgrading to VPN-1 NGX R65	56
	Upgrade Guidelines	56
	Upgrade Order	57
	Upgrade Export/Import	57
	Upgrading via SmartUpdate	58
	VPN-1 Backward Compatibility	59
	Supported Versions	59
	Licensing VPN-1	61
	Obtaining Licenses	61
	Supported Upgrade Paths	63
	Contract Verification	63

Performing License Upgrade.....	65
Pre-Upgrade Considerations	67
Pre-Upgrade Verification Tool	67
Web Intelligence License Enforcement	67
Upgrading on SecurePlatform.....	68
Upgrading SmartCenter Server.....	69
Using the Pre-Upgrade Verification Tool	69
Gateway Upgrade.....	72
Gateway Upgrade with SmartUpdate	72
Review.....	73
Review Questions.....	73
Review Answers	74

Chapter 3 Encryption and VPNs 77

Securing Communication.....	79
Privacy.....	79
Symmetric Encryption	80
Symmetric Disadvantages.....	81
Asymmetric Encryption	82
Diffie-Hellman.....	82
Integrity.....	84
Authentication	85
Two Phases of Encryption	87
Encryption Algorithms.....	88
IKE.....	89
ISAKMP	89
Oakley.....	89
ISAKMP/Oakley	89
Phase 1	90
Phase 2	91
IKE Example.....	92
Tunneling-Mode Encryption.....	93
Certificate Authorities.....	95
Certificates.....	95
Multiple Certificate Authorities	96
Certificate Authority Hierarchy.....	96
Local Certificate Authority.....	98
CA Service via the Internet.....	99
Internal Certificate Authority	100

CA Public Keys	100
Creating Certificates	102
Review	105
Review Questions	105
Review Answers	106
Chapter 4 Introduction to VPNs	107
The Check Point VPN	109
How a VPN Works	111
Specifying Encryption	112
VPN Deployments	114
Site-to-Site VPNs	114
Remote-Access VPNs	115
VPN Implementation	117
Three Critical VPN Components	117
VPN Setup	118
How a VPN Works	120
VPN Communities	122
VPN Topologies	124
Choosing a Topology	125
Authentication Between Community Members	129
Dynamically Assigned IP Gateways	131
Routing Traffic Within a VPN Community	131
Access Control and VPN Communities	132
Excluded Services	134
Special Considerations for Planning a VPN Topology	134
Authorizing Control Connections in VPN Communities	135
Integrating VPNs into a Rule Base	138
Review	141
Review Questions	141
Review Answers	142
Chapter 5 Site-to-Site VPNs	143
Site-to-Site VPN	145
Domain-Based VPN	145
Route-Based VPN	147
VPN Routing Process for VTIs	147
Routing Multicast Packets Through VPN Tunnels	151

VPN Tunnel Management	153
Permanent Tunnels	153
VPN Tunnel Sharing	157
Wire Mode	159
Wire Mode in a MEP Configuration	160
Wire Mode with Route-Based VPN	161
Wire Mode Between Two VPN Communities	162
Directional VPN Enforcement	164
Directional Enforcement Between Communities	166
Multiple Entry Point VPNs	168
VPN High Availability with MEP	168
Traditional Mode VPNs	169
Lab 2: Two-Gateway IKE Encryption (Shared Secret)	171
Lab 3: Two-Gateway IKE Encryption (Certificates)	195
Review	207
Review Questions	207
Review Answers	208

Chapter 6 Remote Access VPNs 209

Remote Access VPN	211
Extending SecuRemote with SecureClient	212
Connect Mode	213
Establishing Remote Access — Workflow	214
Office Mode	215
How Office Mode Works	216
Office Mode Planning	218
IP Pool vs. DHCP	218
Routing-Table Modifications	218
Multiple External Interfaces	218
Before Configuring Office Mode	219
Desktop Security Policy	220
Policy Expiration and Renewal	220
Policy Server HA	221
Wireless Hotspot/Hotel Registration	221
Logging	222
SecureClient Mobile	222

VPN Routing — Remote Access	224
Hub Mode	225
SSL Network Extender	227
How SSL Network Extender Works	228
Prerequisites	228
Clientless VPN	231
Special Considerations for Clientless VPN	234
Configuring Clientless VPN	235
Creating Appropriate Rules in the Rule Base	235
Lab 4: Configuring Remote Access in an IKE VPN	237
Lab 5: Using SecuRemote in an IKE VPN	247
Lab 6: Remote Access and Office Mode	259
Lab 7: SSL Network Extender	273
Review	287
Review Questions	287
Review Answers	288

Chapter 7 High Availability and ClusterXL

Management High Availability	293
Management High Availability Environment	295
Synchronization Status	295
ClusterXL	298
Load Sharing	300
ClusterXL Modes	301
Legacy High Availability Mode	301
New High Availability Mode	302
Load Sharing Multicast Mode	304
Load Sharing Unicast (Pivot) Mode	304
Cluster Control Protocol	307
Synchronizing Clusters	309
The Synchronization Network	309
How State Synchronization Works	310
Synchronized-Cluster Restrictions	311
Sticky Connections	313
The Sticky Decision Function	313
CPHA Commands	315
cphastart	315

cphastop.....	315
cphaprob.....	315
cphaprob Example.....	317
fw hastat.....	320
Debugging ClusterXL Issues.....	321
fw ctl pstat Sync Output.....	322
ClusterXL Configuration Issues.....	324
Modes of ClusterXL Supporting SecureXL.....	324
Crossover-Cable Support.....	324
Lab 8: Deploying New Mode HA.....	325
Lab 9: Load Sharing Unicast (Pivot) Mode.....	349
Lab 10: Configuring Load Sharing Multicast Mode (Optional).....	355
Review.....	365
Review Questions.....	365
Review Answers.....	366
Appendix 1: VPN-1 Distributed Installation.....	369
Appendix 2: Configuring VPN-1 Using the CLI.....	399
Appendix 3: Creating Objects, Establishing Trust and Configuring SmartMap.....	409
Appendix 4: Configuring the Security Policy.....	429

