

CONTENTS

.....	
1	Check Point Security Administration NGX II 1
	Course Objectives 1
	Course Layout 2
	Prerequisites 2
	Check Point Certified Security Expert (CCSE) 2
	Recommended Setup for Labs 3
2	Installing VPN-1 NGX and Upgrading 9
	Objectives 9
	Key Terms 10
	Preinstallation Configuration 11
	Distributed Installation 12
	Upgrading To NGX 13
	Upgrade Guidelines 13
	Upgrade Order 14
	Upgrade Export / Import 14
	Upgrading via SmartUpdate 15
	NGX Backward Compatibility 16
	Supported Versions 16
	Licensing NGX 17
	Obtaining Licenses 17
	Deploying Licenses 18
	Upgrading Licenses to NGX 22
	Licensing and Troubleshooting 23
	Viewing Licenses in User Center 23
	Viewing Licenses in SmartView Monitor 24
	Lab 1: NGX Distributed Installation 27
	Lab 2: Installing VPN-1 Pro Gateway on SecurePlatform Pro 45
	Lab 3: Upgrading NG with AI R55 to NGX 55

▪
▪
▪
▪
▪

SmartCenter Server Pre-Upgrade Overview	67
Pre-Upgrade Verification-Tool Syntax	67
SmartCenter Server Upgrade	68
SmartCenter High Availability Upgrade	68
SecurePlatform Upgrade	68
Advanced Upgrade	72
Upgrading on Windows	74
Security Gateway Upgrade	75
Clustered Deployment Upgrade	75
SmartUpdate Upgrade	75
SmartUpdate Upgrade	77
SecurePlatform R54, R55, and Later Upgrade	78
SecurePlatform NG FP2, FP3, or FP3 Edition 2 Upgrade	80
Upgrading Gateway on Windows	82
Lab 4: Upgrading NG with AI Security Gateway via SmartUpdate	85
Review	89
Review Questions	89
Review Answers	91
3 Advanced NGX Management Concepts	93
Objectives	93
Key Terms	94
Advanced Rule Base Functions	95
Object Cloning	95
Lab 5: Creating Objects Using Object Cloning	97
Rule Base Management	101
Database-Revision Control and Policy Package Management	103
Database Revision Control	103
Policy Package Management	103
Lab 6: Using Database Revision Control	107
Management High Availability	115
Primary vs. Secondary	115
Active vs. Standby	116
Restrictions	116
Synchronization	117

·
·
·
·

Lab 7: Deploying Management HA	121
Review	131
Review Questions	131
Review Answers	133

4 Administrative Utilities	135
Objectives	135
Key Terms	136
Protocol Analyzers Overview	137
NGX fw monitor	138
Lab 8: Capturing Information with fw monitor	147
NGX Debug Commands	151
fw ctl pstat	154
fw ctl debug	160
Using the fw tab command	164
Debug Mode with fwd	165
Debugging cpd Process	169
OPSEC Related Issues	169
General cpd Issues	169
Redirecting Output	169
The cpinfo File	170
VPN Debugging Tools	176
SecureClient Debugging Tools	179
Debugging Logging	182
Lab 9: Using fw ctl pstat	185
Lab 10: Using cpinfo	187
Review	193
Review Questions	194
Review Answers	195

5	Check Point QoS	197
	Objectives	197
	Key Terms	198
	Check Point QoS Overview	199
	Check Point QoS Architecture	200
	Check Point QoS Deployment Considerations	201
	Check Point QoS Policy	202
	Check Point QoS Rule Base	203
	QoS Action Properties	204
	Bandwidth Allocation and Rules	206
	Differentiated Services	220
	DiffServ Markings for IPSec Packets	220
	Interaction Between DiffServ Rules and Other Rules	220
	Low Latency Queuing	222
	Low Latency Classes	222
	Low Latency Class Priorities	224
	When to Use Low Latency Queueing	227
	Advanced Features	228
	Authenticated QoS	228
	Citrix MetaFrame Support	228
	Load Sharing	229
	Monitoring QoS Policy	230
	SmartView Tracker	230
	SmartView Monitor	231
	Eventia Reporter	232
	Optimizing Check Point QoS	233
	Lab 11: Configuring Check Point QoS Policy	235
	Review	245
	Review Questions	245
	Review Answers	247

- 6 Enabling Voice Over IP Traffic 249**
 - Objectives 249
 - Key Terms 250
 - Voice Over IP Basics 251
 - Supported Protocols 253
 - Configuring NGX for H.323-based VoIP Traffic 255
 - Enabling VoIP Traffic in an H.323 Environment 256
 - Gatekeeper Object Configuration 256
 - Configuring Gatekeeper Routing Mode 258
 - Gateway Object Creation (Optional) 259
 - Configuring Gateway Routing Mode 260
 - Configuring Global Properties 262
 - Configuring the Rule Base for H.323 Traffic 263
 - Enabling VoIP Traffic in a SIP Environment 265
 - Defining the VoIP SIP Domain 267
 - Configuring Global Properties 268
 - Configuring the Rule Base for SIP Traffic 269
 - SIP Services 271
 - Lab 12: Configuring Security Policy for VoIP Communications 273
 - Review 285
 - Review Questions 285
 - Review Answers 287

- 7 ClusterXL 289**
 - Objectives 289
 - Key Terms 290
 - High Availability 291
 - Load Sharing 293
 - State Synchronization 298
 - CPHA Commands 300
 - cphastart 300
 - cphastop 300
 - cphaprob 300
 - fw hastat 304

▪
▪
▪
▪
▪

Debugging ClusterXL Issues	305
ClusterXL Configuration Issues	308
Lab 13: Deploying New Mode High Availability	309
Lab 14: Manual Failover (Optional)	323
Lab 15: Configuring Load Sharing Unicast (Pivot) Mode	325
Lab 16: Configuring Load Sharing Multicast Mode (Optional)	329
Review	333
Review Questions	333
Review Answers	335

8 Advanced VPN 337

Objectives	337
Key Terms	338
SecureClient	339
Network Configuration	343
Licensing	347
SecureClient Policy	348
Installing Desktop Policies	349
Lab 17: Configuring the Policy Server	351
VPN Routing	361
VPN Routing with DAIP	362
Remote-Access Clients and VPN Routing	363
Security and Connectivity	363
Remote Client to Remote Client	364
DAIP Environment	365
Hub / Satellite Environment	365
SecuRemote / SecureClient Environment	366
Lab 18: Configuring VPN Routing	369
Route-Based VPN	377
Example	377
VPN Tunnel Interface	379
Numbered / Unnumbered VTIs	381
Configuring VTIs	381
Directional VPN Rule Match	384

▪
▪
▪
▪

Dynamic VPN Routing	387
Configuring Dynamic VPN Routing Using OSPF	387
Wire Mode in Route-Based VPN	391
How Wire Mode Works	391
Wire Mode in Route-Based VPN	395
Lab 19: Route-Based VPN Using Static Routes	397
Lab 20: Dynamic VPN Routing	
Using OSPF	405
Review	417
Review Answers	419

•
•
•
•
•