

# CONTENTS

.....	
<b>1</b>	<b>Check Point Security Administration NGX I ..... 1</b>
	Course Objectives ..... 1
	Course Layout ..... 2
	Prerequisites ..... 2
	Check Point Certified Security Administrator (CCSA) ..... 2
	Exam-Number Note: 156-215.1 ..... 3
	Revision Differences ..... 4
	Recommended Setup for labs ..... 5
	What's New in VPN-1 NGX ..... 11
	Security-Management Cost Reduction ..... 11
	Network and Application Security ..... 12
	VPN Management ..... 12
	For More Information ..... 13
<b>2</b>	<b>VPN-1 NGX Overview ..... 15</b>
	Objectives ..... 15
	Key Terms ..... 16
	VPN-1 NGX Architecture ..... 17
	SmartConsole and SmartDashboard ..... 17
	SmartCenter Server ..... 18
	Security Gateway ..... 18
	How VPN-1 NGX Works ..... 20
	The INSPECT Engine ..... 20
	Distributed Deployments ..... 23
	SVN Foundation ..... 24
	Secure Internal Communications (SIC) ..... 24
	SmartConsole Components ..... 28
	SmartDashboard ..... 28
	SmartView Tracker ..... 31

·  
·  
·  
·  
·

SmartView Monitor .....	33
Eventia Reporter .....	35
Lab 1: NGX Stand-Alone Installation .....	37
Review .....	57
Review Questions .....	57
Review Answers .....	59

**3 The Security Policy ..... 61**

Objectives .....	61
Key Terms .....	62
Security Policy Defined .....	63
What Is a Security Policy? .....	63
Security Policy Considerations .....	63
Rule Base Defined .....	64
Lab 2: Launching SmartDashboard .....	65
Lab 3: Defining Basic Objects .....	69
Detecting IP Spoofing .....	93
Configuring Anti-Spoofing .....	93
Multicasting .....	97
Configuring Multicast Access Control .....	97
Interface Properties Multicast Restrictions .....	100
IGMP .....	100
Multicast Routing Protocols .....	100
Multicast Traffic .....	101
Creating the Rule Base .....	102
Basic Rule Base Concepts .....	102
The Default Rule .....	102
Basic Rules .....	104
Implicit/Explicit Rules .....	105
Control Connections .....	107
Completing the Rule Base .....	110
Understanding Rule Base Order .....	110
Lab 4: Configuring Anti-Spoofing Measures .....	111
Lab 5: Defining Basic Rules .....	119
Security Policy Command-Line Options .....	131

·  
·  
·  
·

cpstart .....	131
cpstop .....	131
fw Commands .....	132
Advanced Rule Base Functions .....	133
Object Cloning .....	133
Lab 6: Creating Objects Using Object Cloning .....	135
Rule Base Management .....	139
Database Revision Control and Policy Package Management .....	141
Database Revision Control .....	141
Policy Package Management .....	141
Lab 7: Using Database Revision Control .....	145
Review .....	161
Review Questions .....	161
Review Answers .....	163

<b>4 Monitoring Traffic and Connections .....</b>	<b>165</b>
Objectives .....	165
Key Terms .....	166
SmartView Tracker .....	167
SmartView Tracker Login .....	167
Log Types .....	168
SmartView Tracker Views .....	169
Log-File Management .....	171
Administrator Auditing .....	171
Global Logging and Alerting .....	172
Time Settings .....	174
Blocking Connections .....	176
Terminating Active Connections .....	176
Lab 8: Blocking Intruder Connections .....	179
SmartView Monitor .....	189
SmartView Monitor Login .....	189
Key Features .....	190
Monitoring Suspicious Activity Rules .....	190
Monitoring Alerts .....	191
Monitoring Gateways .....	191

•  
•  
•  
•  
•

Monitoring Traffic or Counters .....	192
Monitoring Tunnels .....	192
Monitoring Remote Users .....	193
Lab 9: Setting Up Suspicious Activity Rule in SmartView Monitor .....	195
Lab 10: Checking Status in SmartView Monitor .....	207
Eventia Reporter .....	217
Report Types .....	219
Eventia Reporter Standard Reports .....	220
Eventia Reporter Express Reports .....	220
Predefined Reports .....	221
Eventia Reporter Considerations .....	223
Log-Consolidation Process .....	223
Stand-Alone vs. Distributed Deployments .....	224
Log Availability vs. Log Storage/Processing .....	224
Log-Consolidation Considerations .....	225
Report-Generation Considerations .....	225
Eventia Reporter Database Management .....	228
Database Tuning .....	228
Database-Configuration Modifications .....	229
Database-Size Maintenance .....	230
Backing Up .....	231
Eventia Reporter Licensing .....	232
Review .....	233
Review Questions .....	233
Review Answers .....	235
<b>5 SmartDefense .....</b>	<b>237</b>
Objectives .....	237
Key Terms .....	238
Active Defense .....	239
Components of SmartDefense .....	239
SmartDefense Capabilities .....	240
SmartDefense in Action .....	242
Anti-Spoofing Configuration Status .....	242
Denial-of-Service Attacks .....	242

•  
•  
•  
•

IP and ICMP .....	243
TCP .....	244
Successive Events .....	247
Web Intelligence .....	248
Centralized Control Against Attacks .....	252
Online Updates .....	253
SmartDefense Storm Center .....	254
Storm Center Integration .....	255
Planning Considerations .....	258
Lab 11: Configuring SmartDefense .....	259
Review .....	277
Review Questions .....	277
Review Answers .....	279

**6 Network Address Translation ..... 281**

Objectives .....	281
Key Terms .....	282
Understanding Network Address Translation .....	283
IP Addressing .....	283
Dynamic (Hide) NAT .....	284
Static NAT .....	286
Configuring NAT .....	287
Global Properties .....	288
Dynamic NAT Object Configuration .....	291
Static NAT Object Configuration .....	295
Manual NAT .....	297
When to Use Manual NAT .....	297
Configuring Manual NAT .....	298
Special Considerations .....	299
Lab 12: Configuring Hide NAT .....	301
Lab 13: Configuring Static NAT .....	309
Review .....	319
Review Questions .....	319
Review Answers .....	321

7	<b>Encryption and VPNs</b>	<b>323</b>
	Objectives	323
	Key Terms	324
	How Encryption Works	325
	Privacy	325
	Symmetric Encryption (Shared Key)	326
	Asymmetric Encryption	328
	Diffie-Hellman	328
	Message Integrity	330
	Two Phases of Encrypted Communication	332
	IKE Encryption Scheme	333
	Encryption Algorithms	333
	Tunneling-Mode Encryption	334
	Lab 14: Encryption Demonstration	337
	Review	345
	Summary	345
	Review Questions	345
	Review Answers	346
8	<b>Authentication</b>	<b>347</b>
	Objectives	347
	Key Terms	348
	Understanding Authentication	349
	User Authentication	349
	Session Authentication	349
	Client Authentication	350
	Authentication Types	350
	Authentication Schemes	351
	User Authentication	352
	Client Authentication	353
	How Client Authentication Works	353
	Sign-On Methods	354
	Lab 15: Defining User Templates	359
	Lab 16: Setting Authentication Parameters (Optional)	371
	Lab 17: Defining Users	375

·  
·  
·  
·

Lab 18: Configuring User Authentication .....	383
Lab 19: Configuring Client Authentication .....	395
Review .....	407
Review Questions .....	407
Review Answers .....	409

**9 LDAP User Management with SmartDirectory ..... 411**

Objectives .....	411
Key Terms .....	412
LDAP Servers .....	413
Introduction to Account Management .....	413
LDAP Features .....	414
Multiple LDAP Servers .....	416
Integrating LDAP with VPN-1 NGX .....	417
Exporting Users .....	417
Using an Existing LDAP Server .....	419
Managing LDAP Users .....	420
Organizational Units .....	420
Before Starting Account Management .....	420
Deleting an Object Tree .....	421
Defining Users .....	421
LDAP and SmartDashboard Troubleshooting .....	422
LDAP Issues .....	422
Schema Checking .....	423
SmartDashboard Issues .....	424
NGX Issues .....	426
Important Debugging Tools .....	427
Lab 20: Configuring LDAP Authentication with SmartDirectory .....	429
Review .....	437
Review Questions .....	437
Review Answers .....	439

•		
•		
•		
•		
•		
<b>10 Disaster Recovery</b>		<b>441</b>
Objectives		441
Key Terms		442
Backing Up for Disaster Recovery		443
\$FWDIR/conf		443
\$FWDIR/lib		443
Log Files		443
objects.C and objects_5_0.C		444
rulebases_5_0.fws		444
fwauth.NDB		444
Exporting User Database Only		445
Backing Up Using Export		446
Lab 21: Backup and Restore		447
Review		457
Review Questions		457
Review Answers		459
<b>Appendix A: Attack-Prevention Safeguards</b>		<b>461</b>
<b>Appendix B: Backup and Restore</b>		<b>467</b>