

CONTENTS

.....	
1	Accelerated CCSE NGX	1
	Course Objectives	1
	Course Layout	2
	Prerequisites	2
	Exam-Number Note: 156-915.1	3
	Revision Differences	4
	Recommended Setup for Labs	5
2	Installing VPN-1 NGX and Upgrading	11
	Objectives	11
	Key Terms	12
	Preinstallation Configuration	13
	Distributed Installation	14
	Upgrading To VPN-1 NGX	15
	Upgrade Guidelines	15
	Upgrade Order	16
	Upgrade Export/Import	16
	Upgrading via SmartUpdate	17
	NGX Backward Compatibility	18
	Supported Versions	18
	Licensing VPN-1 NGX	19
	Obtaining Licenses	19
	Deploying Licenses	20
	Upgrading Licenses to VPN-1 NGX	24
	Licensing and Troubleshooting	25
	Viewing Licenses in User Center	25
	Viewing Licenses in SmartView Monitor	26
	SmartCenter Server Pre-Upgrade Overview	29
	Pre-Upgrade Verification-Tool Syntax	29

•
•
•
•
•

SmartCenter Server Upgrade	30
SmartCenter High Availability Upgrade	30
SecurePlatform Upgrade	30
Advanced Upgrade	33
Upgrading on Windows	35
Security Gateway Upgrade	36
Clustered-Deployment Upgrade	36
SmartUpdate Upgrade	36
Upgrading a Gateway Using SmartUpdate Upgrade	38
SecurePlatform R54, R55, and Later Upgrade	39
SecurePlatform NG FP2, FP3, or FP3 Edition 2 Upgrade	41
Upgrading Gateway on Windows	43
Lab 1: Upgrading NG with AI R55 to NGX	45
Lab 2: Upgrading NG with AI	
Security Gateway via SmartUpdate (Optional)	59
Lab 3: NGX Distributed Installation	65
Lab 4: Installing VPN-1 Pro Gateway on SecurePlatform Pro	85
Review	99
Review Questions	99
Review Answers	101
3 Advanced NGX Management Concepts	103
Objectives	103
Key Terms	104
Advanced Rule Base Functions	105
Object Cloning	105
Lab 5: Creating Objects Using Object Cloning	107
Database Revision Control and Policy Package Management	111
Database Revision Control	111
Policy Package Management	111
Lab 6: Using Database Revision Control	115
Review	125
Review Questions	125
Review Answers	126

•
•
•
•
•

4	Configuring Remote Access	127
	Objectives	127
	Key Terms	128
	VPN-1 SecuRemote/SecureClient	129
	Using SecuRemote	129
	Configuring SecuRemote	130
	Rule Base Configuration	131
	Configuring a Remote-Access VPN	133
	Configuring a Remote Access VPN Community	133
	Remote-Access Community Properties	134
	Global Properties Settings	137
	Remote-Access Settings	137
	Client Authentication	151
	Structure of a SecuRemote Connection	152
	Topology	152
	Authentication	152
	Key Exchange	152
	Connection	153
	Routing Considerations	153
	Lab 7: Configuring Remote Access in an IKE VPN	155
	Lab 8: Installing SecuRemote	167
	Advanced Configurations	177
	Secure Domain Login	177
	Authentication by IP Address	177
	SecuRemote Client	178
	Lab 9: Using VPN-1 SecuRemote in an IKE VPN	179
	The SecureClient GUI	191
	Authentication Screen	191
	SecureClient Settings Screen	192
	The Taskbar Menu	199
	Enabling/Disabling Desktop Policies	201
	Retrieving Desktop Policies from Policy Servers	202
	Obtaining Site Topology	203
	userc.C	203
	Overlapping VPN Domains	205
	SecureClient Icon	206

▪
▪
▪
▪
▪

Passwords	207
Auto Local Logon	207
Configuring Auto Local Logon	208
Disabling Auto Local Logon	209
SecureClient Considerations	211
Modifying Network Configuration	211
Multiple Adapters	211
SecureClient Files	211
Upgrading SecureClient	212
SecureClient Diagnostics Tool	213
Diagnostic Viewer	213
Policy Viewer	215
SmartView Tracker	216
Partial Topology Configuration	218
Connect Mode	219
Connection Profiles	219
Office Mode	221
Overview	221
How Office Mode Works	222
Office Mode by RADIUS Server	225
DHCP Enhancements	228
Office Mode per User	229
Office Mode per Site	233
Office Mode per IP Range	235
Routing Considerations	238
Lab 10: Office Mode	241
Review	255
Review Questions	255
Review Answers	256
5 Monitoring Traffic and Connections	257
Objectives	257
Key Terms	258
SmartView Tracker	259
SmartView Tracker Login	259

	▪
	▪
	▪
	▪
	▪
Log Types	260
SmartView Tracker Views	261
Log-File Management	263
Administrator Auditing	263
Global Logging and Alerting	264
Time Settings	266
Blocking Connections	268
Terminating Active Connections	268
Lab 11: Blocking Intruder Connections	271
SmartView Monitor	279
SmartView Monitor Login	279
Key Features	280
Monitoring Suspicious Activity Rules	280
Monitoring Alerts	281
Monitoring Gateways	281
Monitoring Traffic or Counters	282
Monitoring Tunnels	282
Monitoring Remote Users	283
Lab 12: Setting Up Suspicious Activity Rule in SmartView Monitor	285
Lab 13: Checking Status in SmartView Monitor	297
Eventia Reporter	307
Report Types	309
Eventia Reporter Standard Reports	310
Eventia Reporter Express Reports	310
Predefined Reports	311
Eventia Reporter Considerations	313
Log-Consolidation Process	313
Stand-Alone vs. Distributed Deployments	314
Log Availability vs. Log Storage/Processing	314
Log-Consolidation Considerations	315
Report-Generation Considerations	315
Eventia Reporter Database Management	318
Database Tuning	318
Database-Configuration Modifications	319
Database-Size Maintenance	320
Backing Up	321

·
·
·
·
·

Eventia Reporter Licensing	322
Review	323
Review Questions	323
Review Answers	325

6 LDAP User Management with SmartDirectory327

Objectives	327
Key Terms	328
LDAP Servers	329
Introduction to Account Management	329
LDAP Features	330
Multiple LDAP Servers	332
Integrating LDAP with VPN-1 NGX	333
Exporting Users	333
Using an Existing LDAP Server	335
Managing LDAP Users	336
Organizational Units	336
Before Starting Account Management	336
Deleting an Object Tree	337
Defining Users	337
LDAP and SmartDashboard Troubleshooting	338
LDAP Issues	338
Schema Checking	339
SmartDashboard Issues	340
NGX Issues	342
Important Debugging Tools	343
Lab 14: Configuring LDAP Authentication with SmartDirectory	345
Review	353
Review Questions	353
Review Answers	355

7 Check Point QoS357

Objectives	357
Key Terms	358

•
•
•
•
•

Check Point QoS Overview	359
Check Point QoS Architecture	360
Check Point QoS Deployment Considerations	361
Check Point QoS Policy	362
Check Point QoS Rule Base	363
QoS Action Properties	364
Bandwidth Allocation and Rules	366
Differentiated Services	381
DiffServ Marks for IPSec Packets	381
Interaction between DiffServ Rules and Other Rules	382
Low Latency Queuing	383
Low Latency Classes	383
Low Latency Class Priorities	386
When to Use Low Latency Queueing	388
Advanced Features	389
Authenticated QoS	389
Citrix MetaFrame Support	389
Load Sharing	390
Monitoring QoS Policy	391
SmartView Tracker	391
SmartView Monitor	392
Eventia Reporter	393
Optimizing Check Point QoS	394
Lab 15: Configuring Check Point QoS Policy	395
Review	405
Review Questions	405
Review Answers	407

8 High Availability and Clustering	409
Objectives	409
Key Terms	410
Management High Availability	411
Primary vs. Secondary	411
Active vs. Standby	412
Restriction	412

▪
▪
▪
▪
▪

Synchronization	413
Lab 16: Deploying Management HA	417
HA and ClusterXL	427
Key Elements	428
Restrictions	428
Load Sharing	429
Load Sharing Multicast Mode	429
Load Sharing Unicast Mode	430
How Pivot Mode Works	431
HA vs. Load Sharing	433
State Synchronization	434
Synchronization Modes	434
Selective Synchronization	435
Timing Issues	435
CPHA Commands	436
cphastart	436
cphastop	436
cphaprob	436
fw hastat	440
Debugging ClusterXL Issues	441
fw ctl pstat Sync Output	442
ClusterXL Configuration Issues	444
Modes of ClusterXL Supporting SecureXL	444
Crossover-Cable Support between Two Cluster Members	444
Lab 17: Deploying New Mode HA	445
Lab 18: Manual Failover (Optional)	461
Lab 19: Configuring Load Sharing Unicast (Pivot) Mode	463
Lab 20: Configuring Load Sharing Multicast Mode (Optional)	469
Review	479
Review Questions	479
Review Answers	481