Check Point™
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

CONTENTS

1 Check Point Security Administration NGX II 1

Course Objectives 1
Course Layout 2
Prerequisites 2
Check Point Certified Security Expert (CCSE) 2
Exam-Number Note: 156-315.1 3
Recommended Setup for Labs 5
Recommended Lab Topology 6
IP Addresses 7
Lab Terms 9
Lab Stations 10

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 Content Security 103
Objectives 103
Key Terms 104
Role of the Security Server 105
Security Server Overview 105
OPSEC 106
Understanding Content Security 108
Content Vectoring Protocol (CVP) 110
Inspection 111
URI Filtering Protocol (UFP) 113
How UFP Works 114

Implementing Content Security 115
Security Considerations 115
URI Filtering 116
Mail — SMTP 117
FTP Security Server 119
Blocking FTP over HTTP for Specific Groups 120
Java and ActiveX Stripping 121
CVP Inspection 121
Resources and the Rule Base 124
Proper Rule Placement 124
Consequences of Incorrectly Configured Rules 125
CVP Load Sharing and Chaining 126
CVP Chaining 127
Implementing the TCP Resource 128
Configuring TCP Security Servers 128
TCP Resource Properties 130
UFP Tab 131
CVP Tab 132
Lab 5: URL Screening by File 133
Review 143
Review Questions 143
Review Answers 145

4 Configuring VPNs 147

Objectives 147
Key Terms 148
IKE 149
Gateway-to-Gateway Configuration 149
Specifying Encryption 150
VPN Deployments 151
Intranet VPNs 151
Remote-Access VPNs 152
VPN Implementation 153
Three Critical VPN Components 153
VPN Setup 155

Understanding VPN Deployment 155
Simplified Intranet Setup 157
VPN Community Principles 157
Integrating VPNs into a Rule Base 158
Lab 6: Two-Gateway IKE Encryption Configuration (Shared Secret) 159
Lab 7: Two-Gateway IKE Encryption Configuration (Certificates) 179
Review 195
Review Questions 195
Review Answers 197

5 Configuring Remote Access 199
Objectives 199
Key Terms 200
VPN-1 SecuRemote/SecureClient 201
Using SecuRemote 201
Configuring SecuRemote 202
Rule Base Configuration 203
Configuring a Remote-Access VPN 205
Configuring a Remote Access VPN Community 205
Remote-Access Community Properties 206
Global Properties Settings 209
Remote-Access Settings 209
Client Authentication 223
Structure of a SecuRemote Connection 224
Topology 224
Authentication 224
Key Exchange 224
Connection 225
Routing Considerations 225
Lab 8: Configuring Remote Access in an IKE VPN 227
Lab 9: Installing SecuRemote 239
Advanced Configurations 249
Secure Domain Login 249
Authentication by IP Address 249
SecuRemote Client 250

Lab 10: Using VPN-1 SecuRemote in an IKE VPN 251
The SecureClient GUI 263
    Authentication Screen 263
    SecureClient Settings Screen 264
    The Taskbar Menu 271
Enabling/Disabling Desktop PolicIES 273
    Retrieving Desktop Policies from Policy Servers 274
Obtaining Site Topology 275
    userc.C 275
    Overlapping VPN Domains 277
SecureClient Icon 278
Passwords 279
    Auto Local Logon 279
    Configuring Auto Local Logon 280
    Disabling Auto Local Logon 281
SecureClient Considerations 283
    Modifying Network Configuration 283
    Multiple Adapters 283
    SecureClient Files 283
    Upgrading SecureClient 284
SecureClient Diagnostics Tool 285
    Diagnostic Viewer 285
    Policy Viewer 287
    SmartView Tracker 288
Partial Topology Configuration 290
Connect Mode 291
    Connection Profiles 291
Office Mode 293
    Overview 293
    How Office Mode Works 294
    Office Mode by RADIUS Server 297
    DHCP Enhancements 300
    Office Mode per User 301
    Office Mode per Site 305
    Office Mode per IP Range 307
    Routing Considerations 310

Lab 11: Office Mode 313
Review 329
Review Questions 329
Review Answers 330

6 Enabling Voice Over IP Traffic 331
Objectives 331
Key Terms 332
Voice Over IP Basics 333
Supported Protocols 334
Configuring VPN-1 NGX for H.323 based VoIP Traffic 336
Enabling VoIP Traffic in an H.323 Environment 337
Gatekeeper-Object Configuration 337
Configuring Gatekeeper Routing Mode 339
Gateway-Object Creation (Optional) 340
Configuring Gateway Routing Mode 341
Configuring Global Properties 342
Configuring the Rule Base for H.323 Traffic 343
Enabling VoIP Traffic in a SIP Environment 345
Defining the VoIP SIP Domain 347
Configuring Global Properties 348
Configuring the Rule Base for SIP Traffic 349
SIP Services 351
Lab 12: Configuring a Gateway for VoIP Communications 353
Review 363
Review Questions 363
Review Answers 365

7 Check Point QoS 367
Objectives 367
Key Terms 368
Check Point QoS Overview 369
Check Point QoS Architecture 370

Check Point QoS Deployment Considerations 371
Check Point QoS Policy 372
Check Point QoS Rule Base 373
QoS Action Properties 374
Bandwidth Allocation and Rules 376
Differentiated Services 391
DiffServ Marks for IPSec Packets 391
Interaction between DiffServ Rules and Other Rules 392
Low Latency Queuing 393
Low Latency Classes 393
Low Latency Class Priorities 396
When to Use Low Latency Queueing 398
Advanced Features 399
Authenticated QoS 399
Citrix MetaFrame Support 399
Load Sharing 400
Monitoring QoS Policy 401
SmartView Tracker 401
SmartView Monitor 402
Eventia Reporter 403
Optimizing Check Point QoS 404
Lab 13: Configuring Check Point QoS Policy 405
Review 415
Review Questions 415
Review Answers 417

8 High Availability and Clustering 419
Objectives 419
Key Terms 420
Management High Availability 421
Primary vs. Secondary 421
Active vs. Standby 422
Restriction 422
Synchronization 423
Lab 14: Deploying Management HA 427

HA and ClusterXL 437
Key Elements 438
Restrictions 438
Load Sharing 439
Load Sharing Multicast Mode 439
Load Sharing Unicast Mode 440
How Pivot Mode Works 441
HA vs. Load Sharing 443
State Synchronization 444
Synchronization Modes 444
Selective Synchronization 445
Timing Issues 445
CPHA Commands 446
cphastart 446
cphastop 446
cphaprob 446
fw hastat 450
Debugging ClusterXL Issues 451
fw ctl pstat Sync Output 452
ClusterXL Configuration Issues 454
Modes of ClusterXL Supporting SecureXL 454
Crossover-Cable Support between Two Cluster Members 454
Lab 15: Deploying New Mode HA 455
Lab 16: Manual Failover (Optional) 471
Lab 17: Configuring Load Sharing Unicast (Pivot) Mode 473
Lab 18: Configuring Load Sharing Multicast Mode (Optional) 479
Review 489
Review Questions 489
Review Answers 491