

Contents

Preface: Check Point NGX (R65) Security Administration on Nokia IP

Security Platforms	i
Course Layout	iv
Course Requirements	iv
Prerequisites	iv
Check Point Certified Security Administrator (CCSA)	v
Certification	v
Recommended Lab Topology	vii
Standard Configuration	vii
IP Addresses	viii
Lab Terms	xii
Check Point Security Architecture	xiii
Unified Security Architecture	xiv
Complete Protection	xv
Broad Range of Security Solutions	xvi
Network Security	xvii
Data Security	xix
Security Management	xx
Services	xxi
Training and Certification	xxii
CCMA	xxiii
Learn More	xxiii

Module 1 Sales Overview	1
The Nokia Complete System Approach	2
Platform Layer	2
Application Layer	3
Management Layer	3
Support Layer	4
Nokia IP Security Platforms	5
Plug-and-Play Implementation	5
Easy Serviceability	5
Routing and Stateful Inspection	6
Remote-Network Management	6
Centralized Management	6
World-Class Routing Functionality	6
High Availability	6
Nokia IP Clustering	7
Nokia IPSO and Network Voyager	8
Nokia IPSO	8
Nokia Network Voyager	8
Nokia Products	10

SOHO Products	12
Nokia IP60	12
Enterprise Products	15
Nokia IP260 and IP265	15
Nokia IP290	17
Nokia IP390	17
Nokia IP560	18
Carrier/xSP Products	20
Nokia IP690 Hardware	20
Nokia IP1220/1260	21
Nokia IP2255	23
Nokia IP2450	24
Module 2 Nokia IPSO	27
Nokia IPSO Operating System	28
IPSO Routing Daemon (IPSRD)	29
IP Clustering in IPSO	30
Command Line Interface (CLI)	32
Disk Mirroring (RAID Level 1)	32
What's New in IPSO 4.x	33
Review: IPSO 4.x	34
Module 3 Initial Configuration	35
Nokia IP Security Platform Configuration	36
Accessing the NSP	37
Connecting to Voyager	38
Boot Manager	40
Adding Passwords	41
Host Name and Admin Password	42
Selecting Voyager Interface	43
Setting Up Interface	44
Module 4 Introduction to Voyager	47
Introduction to Voyager	48
Connecting and Authenticating	48
Navigating within Voyager	50
Accessing Features in Voyager	50
Configuration and Monitor Menus	51
Reset, Apply and Save Frame in Voyager	53
Module 5 Introduction to Voyager	55
IPSO File System and Directory Structure	56
The IPSO/config Directory	57
IPSO /image Directory	58
IPSO File System and Partitions	59
Diskless File System	60

Module 6	Introduction to CLISH	63
	CLISH — IPSO’s Dedicated Configuration Shell	64
	Command-Line Movement and Editing	65
	Command Completion	65
	Command Recall	67
	Command Help	68
	Top Level Commands	69
	CLISH Script Commands	69
Module 7	Interfaces and the Database	73
	IPSO’s Underlying Database	74
	Making Database Changes	75
	Uses of IPSO Configuration	76
	Configuring Interfaces	76
	Configuring Physical Interfaces	78
	Configuring Logical Interfaces	80
	Renaming the Interface	81
	Setting up Remaining Interfaces	83
	Support for Nokia VLAN	85
	VLAN Environments Multiplex N:1	85
Module 8	Typical System Configuration	89
	Configuring Basic System Parameters	90
	Setting the Time	90
	Configuring Host Table	91
	Change the Name of your Appliance	93
	Configuring DNS Settings	93
	Sending Alerts	94
Module 9	Auditing	97
	Using Session-Based Voyager	98
	Advantages of Session-Based Voyager	99
	Advanced Login Options in Voyager	99
	Configuring Voyager Web Access	101
	Voyager Auditing Options	103
Module 10	Static Routes	105
	Adding Static Routes	106
	Static Routes Needed for Path Determination	106
	Adding a Single Static Route	108
	Adding Multiple Static Routes	109
Module 11	DHCP and PPPoE	115
	What is DHCP	116
	BOOTP/DHCP Relay	122
	Extending BOOTP/DHCP using BOOTP Relay	122

	PPPoE	124
Module 12	Diskless Architecture	129
	Nokia IPSO Diskless Architecture	130
	Diskless Systems are Flash-Based	130
	Files are Decompressed on Boot	130
	Run-Time Considerations	131
Module 13	Local Services	133
	Working with Local Services.....	134
	Configuring NTP in Voyager	134
Module 14	Diagnostics Tools	141
	Troubleshooting	142
Module 15	Configuring SSH	149
	Secure Shell Overview	150
	Setting Up SSH	154
	Enabling the SSH Service	155
	Create an SSH Session on an IPSO Client	157
	Create an SSH Session on a Windows Client	157
	Tunneling over SSH From a IPSO/Linux to IPSO	158
	Port Forwarding	160
	Troubleshooting SSH Connections	163
Module 16	Configuring SSL	165
	SSL Protocol	166
	Configuring SSL/TLS in Voyager	168
	Setting Private Key and Certificate	170
Module 17	Maintaining Multiple Configurations	181
	The Config File Structure	182
	Managing Configuration Sets	182
Module 18	Backup, Restore, and Replacement	183
	Making Backups of Nokia IP Security Platform.....	184
	Configuration Sets	184
	Scheduling a Backup Task	187
Module 19	Managing IPSO Images	189

	Upgrading IPSO Version	190
	Upgrade Defined	190
Module 20	Package Installation and Management	197
	Installing Software From Voyager	198
	Installing From the CLI	200
Module 21	Boot Manager	205
	Resetting the Admin Password	206
	Restoring an IPSO Device	208
Module 22	User Management	209
	Creating Accounts Other than “admin”	210
	211
Module 23	Role-Based Administration	213
	Role-Based Administration	214
	Role Creation	214
	Predefined Roles	215
Module 24	AAA Concepts	219
	Overview of AAA	220
	RADIUS and AAA	220
	Nokia and AAA	221
Module 25	Configuring RADIUS	223
	Configuring RADIUS	224
	Monitoring RADIUS Traffic	232
Module 26	Simple HA with VRRP	235
	What Happens When a Gateway Fails?	236
	VRRP and Hot Standby	236
	Simplified VRRP Configuration	242
Module 27	Check Point Clustering	245
	ClusterXL	246
	The Cluster Object	247
Module 28	Monitoring	253

	Monitoring the Nokia IP Security Platform	254
	Monitoring Routing Protocols	254
	Monitoring System Status	256
	Generating Reports	257
	Monitoring Syslog Using Voyager	258
Module 29	UNIX Diagnostics	261
	“ps” Allows You to see Running Processes	262
	Diagnose Resource Problems	263
Module 30	Re-installing the Platform	265
	Reinstall Procedure — Boot Manager	266
	Replacing and Restoring a Failed Unit	267
Module 31	Nokia Technical Support	269
	Nokia Complete System Approach	270
	Nokia Online Technical Support	271
	Registering on Nokia Support Site	272
	Software Downloads	273
	Reporting Problems using Cases	274
	Searching for Solutions	275
	Nokia Knowledge Base	276
	Nokia Technical Assistance Center (TAC)	277
Module 32	VPN-1 Overview	281
	VPN-1 Fundamentals	283
	Check Point’s Security Gateway	285
	Bridge Mode	290
	Bridge Mode and STP	291
	VPN-1 Gateway Inspection Architecture	293
	Security Policy Management	296
	SmartConsole Components	296
	VPN-1 SmartCenter Server	308
	Basic Concepts and Terminology	308
	Using Management Plug-Ins	310
	Securing Channels of Communication	311
	Administrative Login Using SIC	314
	SmartUpdate and Managing Licenses	315
	Understanding SmartUpdate	315
	Overview of Managing Licenses	317
	Contracts/Services	323
	Service Contracts	324
	Working with Contract Files	325
	Review	336
	Review Questions	336
	Review Answers	337

Module 33	Introduction to SecurePlatform	339
	Introduction	341
	SecurePlatform Hardware Requirements and Setup	342
	http://www.checkpoint.com/services/techsupport/hcl/index.html	342
	Hardware Compatibility Testing Tool	342
	Using the Command Line	344
	Basic Linux Commands	344
	Backup and Restore	347
	Viewing Scheduling Status in the WebUI	349
	Restoring the Backup via the Command Line	349
	Restoring Older Versions of SecurePlatform	351
	Scheduling a Backup in the WebUI	352
	Viewing the Backup Log in the WebUI	353
	Generating CPInfo	353
	Critical Check Point Directories	354
	Log Files	354
	objects.C and objects_5_0.C	354
	rulebases_5_0.fws	355
	fwauth.NDB	355
	Exporting User Database Only	355
	Backing Up Using upgrade_export	356
	Managing Your SecurePlatform System	358
	Connecting to SecurePlatform Using Secure Shell	358
	User Management	359
	SecurePlatform Command Shell	360
	SecurePlatform Command Shell	360
	Management Commands	361
	Documentation Commands	362
	System Commands	363
	Snapshot-Image Management	364
	System-Diagnostic Commands	365
	Check Point Commands	366
	Network-Diagnostic Commands	369
	Network-Configuration Commands	370
	User and Administrative Commands	373
	Review	374
	Review Questions	374
	Review Answers	375
Module 34	Introduction to the Security Policy	377
	Security Policy Basics	380
	The Rule Base	380
	Managing Objects in SmartDashboard	381
	SmartDashboard and Objects	382
	Managing Objects	383
	Changing the View in the Objects Tree	385
	Creating the Rule Base	387

Basic Rule Base Concepts	387
Default Rule	387
Basic Rules	389
Implicit/Explicit Rules	391
Control Connections	392
Completing the Rule Base	396
Understanding Rule Base Order	396
Rule Base Management	397
Review	397
Useful Tips	397
Policy Management and Revision Control	399
Policy-Management Overview	400
Policy Packages	401
Installation Targets	403
Querying and Sorting Rules and Objects	404
Database Revision Control	408
Implementing Database Revision Control	408
Network Address Translation	411
IP Addressing	412
Dynamic (Hide) NAT	413
Static NAT	414
Hide Versus Static	414
Choosing the Hide Address in Hide NAT	415
Configuring NAT	415
Dynamic NAT Object Configuration	418
Manual NAT	422
Enabling VoIP Traffic	425
Supported Protocols	426
Session Initiation Protocol	427
H.323	430
Detecting IP Spoofing	437
Configuring Anti-Spoofing	437
Multicasting	440
Configuring Multicast Access Control	440
Review	442
Review Questions	442
Review Answers	443

Module 35 Monitoring Traffic and Connections 445

SmartView Tracker	447
SmartView Tracker Login	448
Log Types	448
SmartView Tracker Tabs	450
Action Icons	452
Log-File Management	453
Administrator Auditing	454
Global Logging and Alerting	454
Time Settings	457

Blocking Connections	459
Terminating and Blocking Active Connections	459
SmartView Monitor	461
SmartView Monitor Login	463
Customizable Views	463
Monitoring Suspicious Activity Rules	470
Monitoring Alerts	470
SmartView Tracker vs. SmartView Monitor	474
Eventia Reporter	476
Report Types	478
Predefined Reports	480
Customizing Predefined Reports	482
Eventia Reporter Considerations	483
Eventia Reporter Licensing	486
Review	487
Review Questions	487
Review Answers	488

Module 36 User Management and Authentication

Module 36 User Management and Authentication	489
Creating Users and Groups in SmartDashboard	491
Introduction to VPN-1 Authentication	492
Introduction to Authentication Methods	492
Authentication Schemes	494
Authentication Methods	497
User Authentication	497
Configuring User Authentication	504
Session Authentication	505
Configuring Session Authentication	506
Client Authentication	507
Configuring Client Authentication	513
Resolving Access Conflicts	515
Configuring Authentication Tracking	516
LDAP User Management with SmartDirectory	517
LDAP Features	517
Multiple LDAP Servers	519
Using an Existing LDAP Server	520
Configuring Entities to Work with VPN-1	520
Managing Users	526
SmartDirectory Groups	527
Review	528
Review Questions	528
Review Answers	529

Module 37 Check Point QoS

Module 37 Check Point QoS	531
Check Point QoS Overview	533
Stateful Inspection	534
Intelligent Queuing Engine	534
Weighted Flow Random Early Drop	534

Retransmission Detection Early Drop	535
Check Point QoS Architecture	536
Basic Architecture	536
QoS SmartCenter Server	536
QoS SmartConsole	537
The Security Gateway	537
Deploying QoS	539
Check Point QoS Topology Restrictions	541
Check Point QoS Rule Base	543
Bandwidth Allocation and Rules	543
Traditional and Express Modes	545
QoS Action Properties	547
Bandwidth Allocation and Subrules	549
Implementing the Rule Base	550
QoS Rule Considerations	551
Differentiated Services	553
DiffServ Marks for IPSec Packets	553
Interaction Between DiffServ Rules and Other Rules	554
Low Latency Queuing	556
Low Latency Classes	556
Low Latency Class Priorities	557
When to Use Low Latency Queuing	561
Authenticated QoS	562
Monitoring QoS Policy	563
SmartView Tracker	563
SmartView Monitor	565
Eventia Reporter	565
Optimizing Check Point QoS	567
Review	568
Review Questions	568
Review Answers	569

Module 38 Basic SmartDefense and Content Inspection

Introducing SmartDefense	573
Networks and Application Intelligence	574
Web Intelligence	575
Online Updates	575
Monitor Only Mode	576
Network Security	578
Denial-of-Service	578
IP and ICMP	580
TCP	580
Fingerprint Scrambling	581
Successive Events	582
DShield Storm Center	583
Port Scanning	585
Application Intelligence	588
Mail	588
FTP	589

Microsoft Networks	590
Peer-to-Peer	590
Instant Messaging	590
DNS	591
VoIP	592
SNMP	592
Web Intelligence	594
Web Intelligence Protections	594
Web Intelligence License Enforcement	596
SmartDefense Services	599
Download Updates Tab	599
Advisories Tab	601
Security Best Practices Tab	603
Content Inspection	604
Introduction to Integrated Antivirus and Web-Filtering Technologies	604
Database Updates	605
Antivirus-Scan Settings	606
Web Filtering	614
Review	616
Review Questions	616
Review Answers	617

