
Contents

Course Objectives	ix
--------------------------------	----

Preface: Multi-Domain Management with Check Point Provider-1 R70	1
Course Layout	2
Provider-1 Course Prerequisites	3
Lab Setup	4
Lab Topology	5
IP Addresses and Classroom Configuration	6
Course and Lab Terminology	8

Chapter 1 Provider-1 R70 Deployment	9
Key Points	10
Key Terms	11
Provider-1 R70 Overview	12
Managed Service Providers	14
Data Centers	16
Enterprises	19
Network Operations Center Security	24
MDG Communication	24
Enhancing NOC Security	24
The Check Point Solution	25
Multi-Domain GUI	28

Multi-Domain Server	29
Remote Security Gateway	34
Basic Provider-1 R70 Configuration	37
Point-of-Presence Provider-1 R70 Configuration	39
NOC Security	41
Log Management	43
Benefits of Provider-1 R70	46
Centralized Management	46
Customer Security	46
Product Scalability	46
Multi-Level High Availability	47
Review	49
Review Questions	50
Review Answers	52
Chapter 2 MDS Installation and Configuration	53
Key Points	54
Key Terms	55
Choosing the Type of MDS	56
MDS — Manager	56
MDS — Container	57
Multi-Domain Server as Multi-Domain Log Module	57
Licensing Provider-1	58
The Trial Period	58
Considerations	58
License Details	60
Replacing the Trial-Period License	62
Upgrading Licenses	63
Provider-1 System Requirements	64
Minimum Hardware Requirements for Provider-1 MDS	64
Minimum Hardware Requirements for Provider-1 MDG and SmartConsole	65
Software Requirements	66
SecurePlatform Appliances	70
IP Allocation and Routing	70
File Structure	72
MDS and CMA Command-Line Options	76

Lab 1: Installing and Configuring the Primary MDS Station .	81
Install SecurePlatform	82
Configure SecurePlatform	86
Install and Configure the Primary MDS	93
Installing the MDG	101
Install the R70 GUIclient	101
Install the Multi-Domain GUIclient.	109
Review.	113
Review Questions.	114
Review Answers	115
Chapter 3 Overview of the Multi-Domain GUI	117
Key Points	118
Key Terms	119
Installing GUI Clients	120
Multi-Domain GUI Functionality	121
Navigating the MDG	122
Selection Bar	123
Provider-1 Administrative Modes	125
Provider-1 Properties	126
General View.	131
Customer Contents Mode	131
MDS Contents Mode	132
Network Objects Mode.	133
General Toolbar Buttons.	136
Global Policy View	140
Security Policies Mode.	140
VPN Communities Mode	141
Administrators View	144
Administrators Toolbar Buttons	146
GUI Clients View	149
GUI Clients Toolbar Buttons	150
SmartUpdate View	152
SmartUpdate Toolbar Buttons.	154
High Availability View	158
Customer Contents Mode	158
MDS Contents Mode	159

High Availability Toolbar Buttons	159
Connected Administrators View.....	162
Connected Administrators Toolbar Buttons	163
Lab 2: Securing the NOC	165
Create a Virtual IP Addressing Scheme.....	167
Use the MDG to Log In to the MDS	168
Adding the NOC Firewall CMA	171
Configure the NOC Customer Management Add-On	180
Establishing Communication with the NOC Security Gateways.....	183
Creating Administrators	201
Setting Up a NOC Firewall for Control Connections	220
Rule Base Configuration	223
Lab 3: Adding the UK_Corp City Site to Provider 1 R70	227
Log In to the MDS	228
Add the UK_Corp Customer	230
Configure the Customer Management Add-On	240
Establishing Communication with the UK_Corp Security Gateway	244
Configure CMA Management Objects	244
Establish SIC Between the UK_Corp CMA and Remote Gateway	250
Configure Gateway Properties	259
Backing Up the UK_Corp CMA	261
Lab 4: Creation and Migration of Existing Japan_Corp Site	263
Determine the Virtual IP Addressing Scheme	264
Create the Japan_Corp Customer and CMA	264
Add the Japan_Corp Customer and CMA	265
Copy the Japan_Corp SmartCenter Server files to the Primary MDS	278
Import Japan_Corp Security Manager Server Files into the Japan_Corp CMA	281
Reconfigure the System-Created CMA Object	283
Reconfigure the Imported Rule Base	287
Backing Up the Japan_Corp CMA	289
Review	291
Review Questions.....	292
Review Answers	293

Chapter 4	Provider-1 Logging Features	295
	Key Points	296
	Key Terms	297
	Log Management	298
	Customer Log Module	299
	Multi-Domain Log Module System	301
	MLM Deployment	302
	Using Eventia Reporter	303
Lab 5: MDS MLM Installation and Configuration		305
	Perform SecurePlatform Installation	306
	Configure SecurePlatform	307
	Install and Configure the MDS	309
	Logging in to the MLM	311
	Configure CMA to Log to the CLM	316
	Install User Database	320
	Configure NOC for Control Connections	322
	Verify Logging	324
	Configure a Second CLM for the Japan_Corp CMA	326
	Review	327
	Review Questions	328
	Review Answers	329
Chapter 5	Assigning Global Policies	331
	Key Points	332
	Key Terms	333
	Global Policy	334
	Global Policy Rules	334
	Global Objects	335
	Global Services	336
	Global Policy Database	336
	Customer History	337
	Global IPS	338
	Configuring IPS in Global SmartDashboard	338
	Subscribing a Customer to the Global IPS Service	340

Modifying IPS from the SmartDashboard of a CMA	341
Global VPNs	342
Configuring a Global VPN	342
Global VPN Communities	343
Lab 6: Creating and Assigning a Global Policy	345
Creating Global Objects and Rules	346
Open the Global SmartDashboard	346
Configure Global CMA objects	348
Configure Global Remote-Client objects	350
Configure Global FTP Server Object	351
Configure Simple Group objects	352
Create Global NETBios and Cleanup Rules	354
Create Remote-Access Rules	356
Configure Global IPS	357
Assign Global Policy	367
Verify Global Policy Configuration	372
Review	375
Review Questions	376
Review Answers	377
Chapter 6 Advanced MDS Functions	379
Key Points	380
Key Terms	381
Migrating Existing Security Management Servers into Provider-1	382
MDS High Availability Features	383
Methodology of MDS Synchronization	383
MDS Synchronization	385
CMA High Availability	387
Security Management Server Backup of a CMA	388
MDS Clock Synchronization	390
Backing Up a CMA	391
MDS Archiving Utilities	392
Archiving Scripts	392
Restoring the MDS	393
Using the mds_restore command	393

Lab 7: Configuring MDS High Availability	395
Install SecurePlatform	396
Install and Configure the Secondary MDS	396
Configure the Secondary MDS	397
Mirroring an Existing MDS	401
Before Beginning MDS Mirroring Procedure	401
Perform Mirroring Procedure	403
Complete CMA Mirroring Process	404
Review	409
Review Questions	410
Review Answers	411
 Glossary	 413
 Appendix A Global Policy Database Synchronization for Management HA	 417
