Check Point R75 Management Essentials – Part 1

Check Point Training Course

Section Heading Index

Module 1 - Networks & Firewalls 3
Module 2 - Check Point Components 18
Module 3 – Firewall Installation 26
Module 4 – SmartCenter Installation 49
Module 5 – Connecting to the SmartCenter 66
Module 6 – Creating Objects 83
Module 7 – Creating Rules and Installing the Security Policy 112
Module 8 – SmartView Tracker 144
Module 9 – SmartView Monitor 164
Module 10 – SmartUpdate 178
Module 11 – Working with the Security Policy 189
Module 12 – Setting up Authentication 221
Module 13 – User Authentication 241
Module 14 – Session Authentication 258
Module 15 – Client Authentication 267
Module 16 – Identity Awareness 292
Module 17 – Network Address Translation 315
Module 18 – IPS 341
Module 19 – Content Security Servers 361
Module 20 - Managing Multiple Firewalls 384
Module 21 – Backups and Recovery 400

Module 1 - Networks & Firewalls 3

1 Securing Networks 5
1.1 All Firewalls are Not Equal 5
1.1.1 Primary Organization Network 5
1.1.2 Hosted Services Network 6
1.1.3 Remote Office Networks 7
1.2 Basic Protocols 7
1.2.1 IP Protocol 7
1.2.2 TCP Protocol 8
1.2.3 UDP Protocol 9
1.2.4 ICMP Protocol 10
1.3 Protection Using Simple Packet Filters 10
1.3.1 Packet Filter Protection 10
1.4 Protection Using Application Proxies 10
1.4.1 Application Proxy Protection 11
1.5 Protection Using Hybrids – Stateful Inpsection 11
1.5.1 Stateful Inspection Protection 11
1.5.2 Building State Tables 12
1.5.3 Check Point Filtering Modules 14
1.5.4 Check Point State Tables 14
2 Basic Network Packet Analysis 16
2.1 Sniffing Packets 16
2.1.1 tcpdump 16
2.1.2 Wireshark 16

Module 2 - Check Point Components 18

1 Check Point Components 20
1.1 Product Overview 20
1.1.1 Securing the Global Organization 20
1.1.2 Perimeter 21
1.1.3 Remote Access 21
1.2 Check Point VPN-1 UTM/Power Components 22
1.2.1 Component Overview 22

© Lezha Publications 2012

1.2.2 SmartCenter 22
1.2.3 VPN-1 Power/UTM Modules/Blades 23
1.2.4 GUI Clients 23
2 **Product Combinations 24**
2.1 Modules/blades 24
2.1.1 Check Point Power-1 24
2.1.2 Check Point UTM-1....24
2.1.3 Check Point UTM-1 Edge 24
2.1.4 Check Point Software Gateways 24
2.1.5 Check Point Software SmartCenter & Gateway Bundles....24
2.2 R70 onwards Products – Blades 25
2.2.1 Check Point Gateway Appliances – Power-1....25
2.2.2 Check Point Gateways – IP Appliances....25
2.2.3 Check Point Gateways – UTM-1 Appliances 25
2.2.4 Check Point Gateways – UTM-1 Edge 25
2.2.5 Check Point Software – Security Gateways Bundles....25
2.2.6 Check Point Gateways – Security Management Bundles....25
2.2.7 Check Point Gateways – EndPoint Security 25
2.2.8 Check Point Gateways – Abra 25

Module 3 –Firewall Installation 26

1 **Check the Status Virtual Machine for fw-Site1 & mgmt-Site1 ....28**
1.1 Check the VM settings for fw-Site1 28
1.1.1 Virtual Machine fw-Site1 28
1.1.2 Machine mgmt-Site1....28
2 **Installing the SecurePlatform Base Build 29**
2.1 Install SecurePlatform (SPLAT) 29
2.1.1 Set Keyboard Layout 30
2.1.2 Set an Administration IP Address 30
2.1.3 Set the Port for Web GUI Access....31
2.1.4 Format the Hard Disk & Reboot....31
3 **Installing Firewall Blades on SecurePlatform....32**
3.1 Configure the Base OS Parameters & Check Point Products 32
3.1.1 Initial Login....32
3.1.2 Run ‘sysconfig’....32
3.1.3 Set the Hostname 33
3.1.4 Set the Domain 33
3.1.5 Set Network parameters for Interface eth3 33
3.1.6 Set Network Parameters for Interface eth2....34
3.1.7 Set the Date and Time 35
3.1.8 Import Check Point Products Configuration 36
3.1.9 Check Point Product Install....36
3.1.10 Select Installation Type....37
3.1.11 Select Check Point Products – Security Gateway 37
3.1.12 Select Check Point Products – Basic Configuration 37
3.1.13 Set the Activation Key for SIC....38
3.1.14 Gateway Reboot....38
4 **SecurePlatform with VPN-1 Installed – Basics 39**
4.1 SecurePlatform Access Level & Shells 39
4.1.1 Initial Debugging – fw unloadlocal 40
4.1.2 CPShell Command List....41
4.1.3 Setting the ‘idle’ Timeout....41
4.1.4 Expert Mode 41
4.2 Understanding ‘cpstop’ Security Risks....42
4.2.1 Testing ‘cpstop’....42
4.2.2 Basic tcpdump – Packets on an Interface....43
4.2.3 Using ‘cpstop –fwflag –default’ 44
4.2.4 Using ‘cpstop –fwflag –proc’ 44
4.2.5 Using ‘fwstop’....45
4.3 Basic Network Scan – Using Superscan....45
4.3.1 Superscan – InitialPolicy....45
4.3.2 Superscan – Defaultfilter....47
4.3.3 Superscan – ‘fw unloadlocal’ No Policy installed 47
4.4 Firewall installation Summary....48

Module 4 – SmartCenter Installation 49

1 **Management Server Virtual Machine....51**
1.1 Virtual Machine Setup mgmt-Site1....51
1.1.1 Set the CDROM Boot Device....51
2 **Installing the Check Point SmartCenter and SmartConsole 52**

2.1 *Install SecurePlatform (SPLAT) for the SmartCenter* 52
2.1.1 *Set Keyboard Layout* 52
2.1.2 *Set an Administration IP Address* 53
2.1.3 *Set the Port for Web GUI Access* 53
2.1.4 *Format the Hard Disk & Reboot* 53
2.2 *Configure the Base OS & Check Point SmartCenter* 54
2.2.1 *Initial Login* 54
2.2.2 *Run 'sysconfig'* 54
2.2.3 *Set the Hostname* 54
2.2.4 *Set the Domain* 55
2.2.5 *Network Parameters* 55
2.2.6 *Set the Date and Time* 55
2.2.7 *Import Check Point Products Configuration* 56
2.2.8 *Check Point Product Install* 56
2.2.9 *Select Installation Type* 57
2.2.10 *Select Check Point Products – Security Gateway* 57
2.2.11 *SmartCenter License* 58
2.2.12 *SmartCenter Administrator* 58
2.2.13 *SmartCenter GUI Clients* 59
2.2.14 *SmartCenter CA & Fingerprint* 69
2.2.15 *SmartCenter Reboot & Check Network Connectivity* 60
2.2.16 *Set the 'expert' Password* 60
2.2.17 *'cpconfig' and 'sysconfig' on the SmartCenter* 61
3 SmartConsole Clients 62
3.1 *Installing the SmartConsole Clients on Host1* 62
3.1.1 *Location and Clients to Install* 62
3.1.2 *Getting the SmartConsole from SPLAT* 64

Module 5 – Connecting to the SmartCenter 66

1 Check Point Configuration 68
1.1 *Check Point Configuration – cpconfig* 68
1.1.1 *'cpconfig' on a SPLAT SmartCenter* 68
1.1.2 *Adding Administrators* 68
1.1.3 *Checking the GUI Client List* 69
1.1.4 *Displaying the SmartCenter Fingerprint* 69
1.1.5 *Moving the Fingerprint File to a Workstation* 69
1.2 *Time, SmartCenter and Firewall* 71
1.2.1 *Install NTP Server on Host1* 71
1.2.2 *Set Time Synchronization for SmartCenter and Firewall* 71
2 Basic SmartDashboard – Connecting to the SmartCenter 73
2.1 *The SmartConsole Clients* 73
2.2 *Initial Login to the SmartCenter* 73
2.2.1 *The SmartCenter Fingerprint* 74
2.2.2 *Check Point Software Blades* 74
2.3 *The SmartDashboard Layout* 75
2.3.1 *Turning Display Areas On/Off* 75
2.3.2 *The Objects List* 75
2.3.3 *SmartDashboard Security Policy Tabs* 76
2.4 *Editing the SmartCenter Object* 76
7.4.1 *Objects Tree* 76
2.4.2 *Comment & Color* 77
2.4.3 *Topology* 77
2.4.4 *Log and Masters* 77
3 Basic Rule Parameters 79
3.1 *Introduction to Rules* 79
3.1.1 *Adding a Rule* 79
3.1.2 *Rule Elements* 79
3.1.3 *Rule number and Name* 79
3.1.4 *Setting Source/Destination* 79
3.1.5 *Setting the VPN Column* 80
3.1.6 *Setting the Service* 80
3.1.7 *Setting the Type of Action* 80
3.1.8 *Setting the Type of Logging* 81
3.1.9 *Gateway Installation – Install On* 81
3.1.10 *Comment Field* 82
3.2 *Starting the Other SmartConsole Clients* 82

Module 6 – Creating Objects 83

1 Object Types 85
1.1 *Object Types* 85

1.1.1 *Creating Objects* 85

1.2 *Network Objects* 86

1.2.1 *Check Point* 86

1.2.2 *Nodes* 87

1.2.3 *Network* 87

1.2.4 *Groups* 87

1.2.5 *Dynamic* 87

1.2.6 *Security Zones* 88

1.2.7 *Others* 88

1.2.8 *VoIP Domains* 88

1.3 *Services, Resources, OPSEC, Users & VPN Communities* 89

1.3.1 *Services* 89

1.3.2 *Resources* 89

1.3.3 *Servers & OPSEC Applications* 89

1.3.4 *Users and Administrators* 90

1.3.5 *VPN Communities* 90

2 Creating the Firewall Object 91

2.1 *Check Point Gateway Object* 91

2.1.1 *Create a New Check Point Gateway* 91

2.1.2 *Set the Hostname and IP address 172.21.1.1* 91

2.1.3 *Set the Color to Red* 92

2.1.4 *Select Check Point Software Blades* 92

2.1.5 *Set Secure Internal Communications* 92

2.1.6 *Changes to the Firewall Tab Option List* 93

2.1.7 *HTTPS Inspection* 93

2.1.8 *SecurePlatform* 94

2.1.9 *Setting Logs And Masters* 94

2.1.10 *Capacity Optimization* 95

3 Breaking SmartCenter and Firewall Communications 97

3.1 *Breaking and Resetting SIC* 97

3.1.1 *Reset SIC on the Firewall* 97

3.1.2 *Test Trust for the Firewall Object in the SmartCenter* 98

3.1.3 *Reset SIC in the Firewall Object* 99

4 Creating General Network Objects 100

4.1 *Creating the Network Type Objects* 100

4.1.1 *Create the Internal Network* 100

4.1.2 *Network Object – Broadcast Address* 100

4.1.3 *Create the DMZ Network* 100

4.1.4 *Create the External Network* 101

4.1.5 *Create the Remote Site2 Network* 102

4.2 *Creating Node Type Objects* 102

4.2.1 *Create the Internal Server adsrv01* 102

4.2.2 *Create the Internal Workstation host1* 103

4.2.3 *Create the DMZ SMTP Server Host* 103

4.2.4 *Create the DMZ Web/FTP Server Host* 103

4.2.5 *Create the Class Room Web Server Host* 104

4.3 *Creating External FTP servers for ftp.hp.com* 105

4.3.1 *Using nslookup* 105

4.3.2 *Creating the FTP Servers – Cloning Objects* 106

4.3.3 *Creating a Group Object* 106

4.3.4 *Create the Classroom Router – Gateway Object* 107

4.4 *Summary of Objects Created* 108

5 Dealing with Anti-spoofing 109

5.1.1 *Setting the Topology – Get Interfaces* 109

5.1.2 *Setting Topology – Get Interfaces with Topology (Anti-spoofing)*

5.1.3 *Making Topology Changes* 109

Module 7 – Creating Rules and Installing the Security Policy............. 112

1 Dealing with Policy Packages 114

1.1 *Policy Packages* 114

1.1.1 *Simplified or Traditional Policy* 114

1.1.2 *Creating a New Policy Package* 114

2 Adding rules 116

2.1 *Adding rules* 116

2.1.1 *Stealth Rule* 116

2.1.2 *Internal Network Out bound Rule* 116

2.1.3 *Cleanup Rule* 116

2.1.4 *Broadcast Junk Rule* 116

2.1.5 *SMTP Inbound Rule* 117

2.1.6 *SMTP Outbound Rule* 117

2.1.7 *Web Inbound Rule* 117

2.1.8 *Firewall Secure Shell Access Rule* 118
2.1.9 *Negating Objects in a Rule* 118
2.2 *Reviewing the rules* 118
2.2.1 *Rule Review - Firewall at Risk from the SMTP Server* 119
2.2.2 *Internal Network at Risk from the SMTP Server* 119
2.2.3 *Adding Rule Section Titles* 120
2.2.4 *Rule Summary* 121
3 Policy Installs 122
3.1 *Installing the Policy* 122
3.1.1 *Verifying the Security Policy* 122
3.1.2 *Correcting the Policy after Verification Failures* 122
3.1.3 *Setting the Policy Targets* 123
3.1.4 *Installing the Policy* 124
3.1.5 *Checking the Firewall Status* 126
3.1.6 *Testing the Rules* 126
3.1.7 *Firewall Existing Connections – Behavior* 127
4 Explicit and Implicit Rules 128
4.1 *Implicit Rules* 128
4.1.1 *Viewing Implied Rules* 128
4.1.2 *Turning Implied Rules Off* 130
4.1.3 *Configuring DNS as an Implied Rule – (Don't)* 132
4.1.4 *Accept ICMP requests* 132
4.2 Rule Base Filtering Order 134
4.3 *Breaking SmartCenter to Firewall Connectivity with Implied rules* ....
4.3.1 *Break SmartCenter to Firewall Connectivity* 134
4.3.2 *SmartCenter Connectivity Recovery - cpstop/cpstart* 135
4.3.3 *SmartCenter Connectivity Recovery – SIC Reset* 137
4.3.4 *SmartCenter Connectivity Recovery – 'fw unloadlocal'* 139
4.3.5 *SmartCenter Connectivity Recovery – 'fw fetch mgmt'* 140
4.4 *SmartCenter and Firewall Services* 141
4.4.1 *Check Point 'FW' Services* 141
4.4.2 *Check Point 'CP' Services* 141
4.4.3 *SmartCenter to Firewall Explicit Rule – (For Safety)* 142
5 Saved Versus the Installed Policy 143
5.1 *Saved Policy* 143
5.2 *Installed Policy* 143

Module 8 – SmartView Tracker 144

1 Generate Traffic Using a Network Scanner 146
1.1 *Scan 172.21.1.254* 146
1.1.1 *Set the IP Address Range to Scan – 172.21.1.254* 146
1.1.2 *Check the Type and Ports to Scan* 146
1.1.3 *Run the Scan* 146
1.1.4 *Check Log Events Generated* 147
2 SmartView Tracker 148
2.1 *Log Tabs, Log, Active, Audit* 148
2.1.1 *Network & Endpoint* 148
2.1.2 *Active* 150
2.1.3 *Management* 151
2.1.4 *Predefined Filters* 152
2.2 *Rotating, Archiving and Exporting Logs* 152
2.2.1 *Rotating Log Files* 152
2.2.2 *Archiving Log Files* 152
2.2.3 *Exporting Log Files* 153
2.2.4 *Fetching Log Files from the Firewall* 153
2.3 *Searching and Custom Filters* 155
2.3.1 *Filter Options* 156
2.3.2 *Doing Simple Searches* 157
2.3.3 *Custom Filters* 158
2.3.4 *View Query Properties* 159
2.4 *Custom Commands* 160
2.4.1 *Adding a Secure Shell Custom Command* 160
2.5 *Log Parameters in the SmartDashboard* 161
2.5.1 *Log Type* 161
2.5.2 *Firewall Object* 161
2.5.3 *SmartCenter* 161
2.5.4 *Policy Global Properties* 162
2.6 *Logging to an Alternative Directory* 163

© Lezha Publications 2012

Module 9 – SmartView Monitor 164

1 SmartView Monitor 166
1.1 Gateway Status 166
1.1.1 Filtered views 166
1.1.2 Gateway Properties 166
1.1.3 Other Objects 166
1.2 SmartCenter Object 167
1.2.1 System Information 167
1.2.2 Licences 167
1.2.3 Certificate Authority 168
1.2.4 Status and Connected Clients 168
1.2.5 Disconnecting SmartConsole Clients 168
1.3 Firewall Object 168
1.3.1 System Information 168
1.4 Threshold Settings 169
1.4.1 Global, None, Custom 169
1.4.2 System Alert Daemon 169
2 SmartView Monitor Traffic Statistics 171
2.1 Traffic Statistics 171
2.1.1 Enable SmartMonitor on the Firewall 171
2.1.2 Generate Some Traffic 172
2.1.3 Traffic & System Counters 172
3 Suspicious Activity Monitoring (SAM) 174
3.1 Suspicious Activity Monitoring and Filter Location 174
3.2 Using SmartView Tracker – Active Log 174
3.2.1 Create a Suspicious Connection 174
3.2.2 View Connection in the SmartView Tracker – Active Tab 174
3.2.3 Select Tools – Block Intruder 175
3.2.4 Kill Connection for three Minutes 175
3.2.5 Test Connection Rejects and Alerts 175
3.2.6 Clear all SAM Connections – 'fw sam –f All –D' 175
3.2.7 Test Connections Work 175
3.3 Using SmartView Monitor – Tools 175
3.3.1 Create a Suspicious Connection 175
3.3.2 View Connection in SmartView Tracker – Active Tab 176
3.3.3 Select Tools and Block Intruder 176
3.3.4 View all SAM rules using SmartView Monitor 176
3.3.5 Delete the SAM Rule 176
3.3.6 Create a New SAM Rule Using SmartView Monitor 176
3.3.7 Test the New SAM Rule 177

Module 10 – SmartUpdate 178

1 Check Point User Center 180
1.1 Logging into the User Center 180
1.1.1 Viewing Account Information 180
1.1.2 Viewing Product information 180
1.1.3 Products and Licenses 181
1.1.4 Contracts File 181
1.2 Creating Licenses 181
1.2.1 Central or Local licenses 181
1.2.2 SmartCenter IP Address 182
1.2.3 Changing Licensed IP Address 182
1.2.4 Full Version Upgrades Require New Licenses 182
1.3 R75 Blade licenses 182
1.3.1 Management Blades 183
1.3.2 Network Security Blades 183
2 SmartUpdate – Managing Licenses 184
2.1 Using SmartUpdate 184
2.1.1 Licenses and Contracts 184
2.1.2 Product and Package Information 185
2.1.3 Generating cpinfo data 186
2.1.4 Adding Licenses & Contracts 187
2.1.5 Attaching and Detaching Licenses 188

Module 11 – Working with the Security Policy 189

1 Policy Revision Control 191
1.1 Database Revision Control 191
1.1.1 Creating Revisions 191
1.1.2 Where are Revisions Stored 192
1.1.3 Viewing Revisions 193

© Lezha Publications 2012

1.1.4 *Rolling Back Revisions* 194

2 Rule Display **197**

2.1 *Rule Display and Policy Interaction* 197

2.1.1 *Hiding Rules* 197

2.1.2 *Disabling Rules* 198

2.2 *Rule Filters* 199

2.2.1 *Object Location – Where Used* 199

2.2.2 *Finding Objects in Rules* 200

3 Dealing with Services **202**

3.1 *Predefined Services and the Inspection Engine* 202

3.1.1 *TCP* 202

3.1.2 *UDP* 204

3.1.3 *ICMP* 205

3.1.4 *RPC* 205

3.1.5 *DCE RPC* 206

3.1.6 *Other* 206

3.1.7 *Basic Filtering & IPS Interaction* 207

3.2 *Creating Services* 208

3.2.1 *Creating a TCP Service and Naming Convention* 208

3.2.2 *Advanced Properties - Session Timeout and Filtering* 208

3.2.3 *Two Service Objects Using the Same Port Number* 209

3.2.4 *Applying the New Service to a Rule* 209

3.3 *Abusing a Standard Service – Tunneling over DNS (TCP)* 210

3.3.1 *IPS Filtering for DNS TCP – Default is Off* 210

3.3.2 *Turn on DNS TCP in the Policy Global Properties* 210

3.3.3 *Edit the Telnet Server Port on www.server.com & host1.site1.com*

3.3.4 *Test the Security Policy – Oops* 211

4 Adding More Rules **213**

4.1 *Current Rules check* 213

4.2 *DNS rule* 213

4.2.1 *Create the DNS Server Objects – Type Host* 214

4.2.2 *Add the DNS Rule* 214

4.2.3 *Add the Internal DNS Servers* 214

4.2.4 *Modify the DNS Rule* 214

4.3 *Outgoing Rule for HP FTP Servers* 214

4.3.1 *Add the FTP Outgoing Rule* 214

4.4 *Restricting the Outgoing Rule* 215

4.4.1 *Modify the Outgoing Rule* 215

4.4.2 *Modify the FTP Outgoing Rule* 215

4.4.3 *Delete the Disabled Outgoing Rule* 215

4.5 *Current Security Policy Rules Check* 215

4.5.1 *Verify and Install the policy* 216

5 Simple Systems Analysis for Rule Evaluation **217**

5.1 *How to Evaluate – 'From A to B allow FTP' when B is your Server* 217

5.2 *How to Solve the Problem of Abusing Ports* 219

Module 12 – Setting up Authentication **221**

1 Creating Administrator Accounts **223**

1.1 *Administrator Accounts* 223

1.1.1 *cpconfig* 223

1.1.2 *SmartDashboard – Administrators* 224

1.1.3 *Administrator Profile* 224

1.1.4 *Admin – Groups* 225

1.1.5 *Administrator Authentication Schemes* 225

1.1.6 *Using Certificates* 225

1.1.7 *Testing Administrator Account* 227

1.2 *Using a RADIUS Server* 227

1.2.1 *Create a RADIUS Server Object* 227

1.2.2 *Create another administrator Use - RADIUS Authentication* 228

2 Creating Firewall Rule Authentication Accounts **230**

2.1 *Users for Firewall Rule Authentication* 230

2.1.1 *Supported Authentication Schemes* 230

2.1.2 *Firewall - Enabled Authentication Schemes* 230

2.1.3 *Access Role and Legacy Users Access* 231

2.1.4 *Creating User Groups* 231

2.1.5 *Creating User Templates* 232

2.1.6 *Creating User Accounts* 234

3 Authentication Processes **237**

3.1 *User Administration Database & Daemons* 237

3.1.1 *fwauth.NDB* 237

3.1.2 *fwauthd.conf* 237

© Lezha Publications 2012

3.1.3 Exporting & Importing the User Database....238
3.2 External User Profiles....238
3.2.1 Match all Users....238
3.2.2 Match by Domain....239
3.3 Authentication and Security Rules....239
3.3.1 User Authentication....240
3.3.2 Session Authentication....240
3.3.3 Client Authentication....240

Module 13 – User Authentication 241

1 User Authentication....243
1.1 User Authentication Daemons & Process....243
1.1.1 Authentication Daemons and Supported Services....243
1.1.2 User Authentication – Policy Global Properties....244
1.1.3 Welcome Message....244
1.2 Authentication Using Telnet....244
1.2.1 Add a telnet Authentication rule....244
1.2.2 Check Rule Properties – Intersect with User Database....245
1.2.3 Installing the Policy and Testing Authentication....245
1.3 Authentication Using http....246
1.3.1 Add an http Authentication rule....246
1.3.2 Check Rule Properties – Allowed http Servers....246
1.3.3 Adding predefined servers....247
1.3.4 Installing the policy and Testing Authentication....247
1.4 Authentication Using FTP....248
1.4.1 Add an Authentication rule....248
1.4.2 Format of User/Password for Authenticating Using FTP....248
1.4.3 Installing the Policy and Testing Authentication....248
1.5 Basic Authentication – Summary....249
1.5.1 Multiple Rules or a Single Rule....249
1.5.2 Removing the Check Point Prompt....249
2 Using Authentication from Internal Networks – Rule clashes....250
2.1 Authentication Behavior – Source IP Address....250
2.1.1 Changing the Behavior – GuiDBedit....250
2.2 Using http for Authentication from Internal Networks....252
2.2.1 Adding the Internal Out http Authentication Rule....252
2.2.2 Reason for Authentication Not Being Enforced....253
2.2.3 Correctly Implementing the Authentication Rules....254
3 User Login Details – tcpdump....255
3.1 Stealing User Login Information....255
3.1.1 Packet trace using tcpdump....255
3.1.2 Packet trace using tcpdump and Wireshark....256

Module 14 – Session Authentication 258

1 Session Authentication....260
1.1 Session Authentication Daemon & Process....260
1.1.1 Authentication Daemon & Supported Services....260
1.2 Installing the Session Agent....260
1.2.1 Agent Install....260
1.2.2 Agent Behavior – Every Connection or Per Session....261
1.2.3 Problems with Agent Access – Port 261....262
1.3 Authentication Using FTP....263
1.3.1 Add an Authentication rule....263
1.3.2 Installing the Policy and Testing Authentication....263
1.3.3 Session Agent Using SSL Encryption....265
1.3.4 Using 'Every request' Authentication....266

Module 15 – Client Authentication.... 267

1 Client Authentication....269
1.1 Client Authentication Daemons & Process....269
1.1.1 Authentication Daemons & Supported Services....269
1.1.2 Client Authentication – Policy Global Properties....269
1.1.3 Welcome Message....270
1.1.4 Client Authentication and the Perimeter Router/Firewall....270
1.2 Client Authentication Details....270
1.2.1 Client Authentication – aclientd, Port 259....270
1.2.2 Client Authentication – ahclientd, Port 900....271
1.2.3 Controlling the Number of Sessions and Time Period....271
1.2.4 Client Authentication Sign On Methods....272

1.3 Authentication Using FTP – Manual Authentication 272
1.3.1 Add an Authentication rule..272
1.3.2 Installing the Policy and Testing FTP Access 273
1.4 Authentication Using Secure Shell...274
1.4.1 Add an Authentication rule..274
1.4.2 Installing the Policy and Testing Secure Shell Access.................274
1.5 Authentication Using a Different Port Number..275
1.5.1 Edit the fwauthd.conf File...275
1.5.2 Test the Authentication Using a Different Port Number 276
1.5.3 Add a Rule to Allow Port 2590 Access to the Firewall 276
1.5.4 Port 259 and 900 Versus a Different Port 277
1.6 Client Authentication Using https 278
1.6.1 Edit the fwauthd.conf File on the firewall.....................................278
2 External User Database – LDAP...279
2.1 LDAP Server – Using Active Directory 279
2.1.1 Check the Details of the AD Server 279
2.1.2 Listing the DN for all Users 279
2.1.3 Create an AD Account for Check Point Firewall Service Access .279
2.1.4 Create an LDAP Account Unit 281
2.1.5 Turn on SmartDirectory for Security Gateways............................284
2.1.6 Create an LDAP User Group 284
2.1.7 Fetching the LDAP Account Unit Tree of Data............................285
2.1.8 Add a Client Authentication Rule for the LDAP Group 286
2.1.9 Test the LDAP Authentication..287
2.1.10 Check Point LDAP Account, Domain Admin or Not 288
2.1.11 Change Privilege Level – Remove Domain Admin 289
2.1.12 Enable LDAP SSL Encryption..290

Module 16 – Identity Awareness...292

1 Current Rules Check...294
1.1 Current Rules...294
1.2 Disable the Legacy Authentication Rules...294
2 Current Objects Check 296
2.1 Current Objects..296
2.1.1 Network Objects..296
2.1.2 Services...297
2.1.3 Servers and OPSEC Applications...297
2.1.4 Users and Administrators...297
3 Identity Awareness..298
3.1 Identity Awareness...298
3.1.1 User Databases 298
3.1.2 AD Query...298
3.1.3 Captive Portal 298
3.1.4 Identity Agent...298
3.2 Enabling Identity Awareness..298
3.2.1 Blade License 298
3.2.2 Check the AD User Account 298
3.2.3 Enabling Identity Awareness on the Gateway Object 299
3.3 Using Identity Awareness with AD Query..301
3.3.1 Check the AD Server Users...301
3.3.2 Security Rules using Active Directory Query 302
3.3.3 Standalone Workstation...303
3.3.4 Domain Member Workstation 303
3.4 Using Identity Awareness with Captive Portal..306
3.4.1 Configuring the Captive Portal...306
3.4.2 Security Rule using Captive Portal 307
3.5 Extending the Rule for Captive Portal 309
3.5.1 Add Telnet and FTP to the Access Role Rule.............................309
3.6 Using Identity Awareness with Identity Agents...309
3.6.1 Type of Agents...309
3.6.2 Deployment of Agents..310
3.6.3 Security Rule using Identity Agent...311

Module 17 – Network Address Translation.. 315

1 Rules Check...317
1.1 Current Rules...317
1.1.1 Create a New Policy using Save As 317
1.1.2 Clean up the Current Rules 317
1.2 Rule Summary before starting Network Address Translation....................317
2 Network Address Translation 319

© Lezha Publications 2012

2.1 Basic Network Address Translation 319
2.1.1 RFC 1918 319
2.1.2 Problems with NAT 319
2.2 NAT Properties......320
2.2.1 Policy Global Properties – NAT 320
2.2.2 Client Side NAT 320
2.2.3 Server Side NAT 321
2.2.4 Objects and the NAT Tab 322
2.3 Hide/Dynamic NAT......323
2.3.1 Hide NAT - Automatic Rules 323
2.3.2 Hide NAT - Manual Rules 323
2.4 Static NAT......324
2.4.1 Static NAT – Automatic Rules......324
2.4.2 Static NAT – Manual Rules......325
2.4.3 Problems with Static NAT – Manual Rules 325
2.4.4 Why does the Firewall need Proxy ARPs 326
2.4.5 Creating Proxy ARPs......326

3 Using Network Address Translation – Basic 327

3.1 Testing a connection without NAT......327
3.1.1 Create a Connection to 172.21.1.254 327
3.1.2 Check the Source Address using 'netstat –a' on 172.21.1.254....327
3.2 Implementing Hide/Dynamic NAT 328
3.2.1 Hide NAT - Automatic Rules 328
3.2.2 Hide NAT - Automatic Rule Testing 328
3.2.3 Hide NAT - Manual Rules 329
3.2.4 Hide NAT - Manual Rules Testing......330
3.3 Implementing Static NAT 330
3.3.1 Static NAT – Automatic Rules......331
3.3.2 State Table ARP Entries – 'fw tab –t arp_table' or 'fw ctl arp'......332
3.3.3 Static NAT – Automatic Rule Testing......333
3.3.4 Static NAT – Automatic Rules, Policy Rule Matching 334
3.3.5 Static NAT – Manual Rules......334

4 Using Network Address Translation – Advanced......337

4.1 Implementing Static NAT and Port Mapping 337
4.1.1 Static NAT – Automatic Rule Problem Using Different Ports 337
4.1.2 Static NAT – Manual Rules with Port Mapping 338
4.2 Hiding a Server on the External Network from the Internet......339
4.2.1 Taking advantage of ARPs 339
4.3 Static NAT without Proxy ARPs, Routed Networks......339

Module 18 – IPS 341

1 IPS and Firewalls......343

1.1 Basic Intrusion Prevention System (IPS) 343
1.1.1 IPS Blade – Requires a License 343
1.1.2 Profile Management......344
1.1.3 Profile Assignment......347
1.1.4 Protections......349

2 IPS Blade Features......350

2.1 Network Security......350
2.1.1 Streaming Engine Settings 350
2.1.2 Anti-Spoofing Configuration Status......351
2.1.3 Denial of Service......351
2.1.4 IP and ICMP 352
2.1.5 TCP......354
2.1.6 Fingerprint Scrambling......354
2.1.7 DShield Storm Center......354
2.1.8 Port Scan 354
2.1.9 NTP......354
2.2 Application Intelligence 355
2.2.1 Mail 355
2.2.2 FTP......356
2.2.3 Microsoft Networks 356
2.2.4 Peer to Peer......356
2.2.5 Instant Messengers 356
2.2.6 DNS 357
2.2.7 VOIP 357
2.2.8 VPN Protocols 357
2.2.9 Remote Control Applications 358
2.2.10 The Others......358
2.3 Web Intelligence......359
2.3.1 Malicious Code 359

2.3.2 Application Layer 360
2.3.3 Information Disclosure 360
2.3.4 HTTP Protocol Inspection 360

Module 19 – Content Security Servers 361

1 Security Policy Rules Check 363
1.1 Create New Policy with Basic Rules 363
2 Content Security Servers 365
2.1 Content Security Servers 365
2.1.1 Servers and Processes, HTTP, FTP, SMTP 365
2.1.2 Resouces (filters) 366
2.1.3 Example Rules 367
3 HTTP Content Security Server 368
3.1 HTTP Resources 368
3.1.1 Creating an HTTP Resource – Query Word Filter 368
3.1.2 Creating an HTTP Resource – Strip Java 370
3.1.3 Creating an HTTP Resource – Block an IP Address 371
3.1.4 Using URI Resources in Rules 372
3.1.5 Testing the Resources 372
3.1.6 URI Match – Example file 373
4 FTP Content Security Server 374
4.1 FTP Resources 374
4.1.1 Creating an FTP Resource 374
4.1.2 Filter Options 374
4.1.3 Apply the Resources to a Rule 375
4.1.4 Testing the Resource 376
5 SMTP Content Security Server 377
5.1 SMTP Resources 377
5.1.1 Creating an SMTP Resource 378
5.1.2 Apply the Resource to a Rule 379
6 CVP and UFP Servers 379
6.1 CVP 379
6.1.1 Creating a CVP Server 379
6.2 UFP 381
6.2.1 Creating a UFP Server 381
6.3 Using OPSEC Groups 382
6.3.1 Creating a Group 382
6.3.2 Load Balancing or Chaining 383

Module 20 - Managing Multiple Firewalls 384

1 Managing Multiple Firewalls 386
1.1 Creating the Virtual Machine 386
1.1.1 Virutal Machine – Type Linux, Red Hat 386
1.2 Installing SecurePlatform 386
1.2.1 Installing SPLAT 386
1.3 Managing Multiple Firewalls 389
1.3.1 SmartCenter License 389
1.3.2 Firewall Module License 389
2 Creating fw.site2.com 390
2.1 Creating fw.site2.com 390
2.1.1 Turn on Logging for Implied Rules 390
2.1.2 Creating the Firewall Object – fw.site2.com 390
2.1.3 Establishing Trust – SIC Communication 391
2.1.4 Topology 391
2.1.5 Writing Rules 392
2.1.6 Installing the Policy 393
2.1.7 Testing the Policy & Generating Log Traffic 394
2.1.8 Log Origin 395
2.2 Managing Multiple Firewalls 396
2.2.1 Single Policy or Multiple Polices 396
2.2.2 Creating Multiple Policies 397

Module 21 – Backups and Recovery 400

1 Backing up the SmartCenter 401
1.1 SmartCenter Configuration - 'upgrade_export' & 'upgrade_import' 401
1.1.1 Using upgrade_export 401
1.1.2 'upgrade_export' and Policy Revisions 403
1.2 Rebuilding a SmartCenter – 'upgrade_import' 404
1.2.1 Building a Virtual Machine for the SecurePlatform SmartCenter .407

© Lezha Publications 2012

1.2.2 Creating a base Install 407

1.2.3 Copying the upgrade_export file cpexport.tgz to SecurePlatform

1.2.4 Completing the Install – Run ‘sysconfig’ 407

1.2.5 Testing the Install...411

1.3 Reset the Environment back to using the Original SmartCenter 412

2 Backing up the Firewall on SecurePlatform...413

2.1 Creating Backups – ‘backup’...413

2.1.1 Create a backup of the Firewall 413

2.1.2 ‘backup’ is just an ‘alias’...414

2.1.3 Setting Automated Backups using the WebGUI 414

2.1.4 Local backup Directory 415

2.2 Recovering a Backup file using ‘restore’ 417

2.2.1 Using Restore to recover a Firewall 417

2.3 Snapshot Images – ‘snapshot’...418

2.3.1 Creating a snapshot...418

2.3.2 The snapshot Directory..419

2.4 Restoring snapshot Images – ‘revert’..419

2.4.1 Restore a snapshot Using ‘revert’..419

3 SPLAT Maintenance Mode 420

3.1 Maintenance Mode – Single User Mode 420

3.1.1 Boot into Maintenance Mode – Single User.................................420