

Contents

Preface: Advanced IPS	1
Advanced IPS Overview	2
Check Point 3D Security	4
Chapter: 1 IPS Management	7
Check Point IPS	8
Learning Objectives:	8
Check Point IPS Overview	9
IPS in SmartDashboard	11
IPS Profiles	14
Activating Protections	21
Protection Browser	23
IPS Updates	29
Network Exceptions	33
Tracking Protections Using Follow Up	34
Geo Protection	35
Bypass Under Load	36
Chapter Review	39
Lab 1: Deploying IPS	41
Configuring the IPS Blade	42
Test the Security Policy and Demonstration Tool	55
Testing IPS Functionality	61
Changing IPS Policy Enforcement	69
Lab 2: Deploying Geo Protection in IPS	77
Modifying Anti-Spoofing Settings	78
Test IPS Geo Protection	83

Chapter: 2 IPS Monitoring	93
Introducing IPS Event Analysis	94
Learning Objectives:	94
IPS Event Analysis	95
IPS Event Analysis Architecture	96
Chapter Review	103
Lab 3: Using Profiles in IPS	105
Testing the Default Protection Profile	106
Define a New Profile	112
Identifying Attacks with SmartEvent	116
Chapter: 3 IPS Architecture	121
Introducing IPS Architecture	122
Learning Objectives:	122
Key IPS Architecture Design Elements	123
Performance — Accelerated Integrated IPS	124
Secure — Multi-threat Detection Engine	125
Passive Streaming Library	126
Protocol Parsers	128
Context Management Infrastructure	129
Compound Signature Identification	131
INSPECTv2	132
How the Architecture Runs IPS	133
Chapter Review	137
Lab 4: Manually Updating IPS Protections (Optional)	139
Downloading and Installing IPS Protections	140
Follow Up with IPS Protection Review	145
Lab 5: IPS Troubleshooting Features	151
Configuring and Testing IPS Troubleshooting Mode	152
Configure and Test the IPS Bypass Settings	167

Chapter: 4 IPS Tuning	175
Optimizing IPS	176
Learning Objectives:	176
Managing Performance Impact	177
Tuning Protections	180
Enhancing System Performance	182
Configure Servers	182
Engine Settings	185
Chapter Review	187
Lab 6: Tuning IPS Performance	189
Configuring Protection Engine Settings	190
Configuring Server Objects	193
Identifying Top Events and Protections	206
Modifying Protections to Defend Against Common Attacks	210
Debugging the Logging Mechanism	215
Chapter: 5 IPS Debugging	219
IPS Debugging	220
Learning Objectives:	220
IPS Debug Tools	221
SmartView Tracker Modes	227
Packet Capture	227
Kernel Debugging	229
IPS Debugging Scenarios	230
False Positives	230
Performance Issues	232
Logging Issues	236
Pattern Match Debug	237
Packet Dump Buffer	237
Debug Flags Overview	238
Chapter Review	239
Lab 7: Advanced IPS Troubleshooting	241
Using Debug to Gather IPS Statistics	242
Using tcpdump to Identify the Source of an Attack	246
Modifying Protection to Prevent Attack Source	248
Viewing Gateway Messages	263

Appendix: Chapter Questions and Answers 265

Chapter 1 - IPS Management	266
Chapter 2 - IPS Monitoring	267
Chapter 3 - IPS Architecture	268
Chapter 4 - IPS Tuning	269
Chapter 5 - IPS Debugging	270