

# Check Point IPS/AV/ABOT Immersion



**Shadow Peak**

*SECURITY TRAINING AND SERVICES*

# Table of Contents

Welcome & Introduction.....	10
Check Point IPS/AV/ABOT Immersion Class Details.....	11
List of Class Modules.....	12
Module 0 – The Basics of Check Point Objects, Policies, & Logging (optional).....	13
Discovery – The Elements of your Check Point Environment.....	15
Objects.....	16
Rules.....	18
Publishing & Installing Policy.....	22
Multiple GUI Administrators - “pencil” and “lock” Icons.....	24
Hit Counts.....	26
Examining Firewall Traffic Logs.....	27
Module 1 – History of IDS/SmartDefense/IPS/AV/ABOT.....	29
The Long Road From Intrusion Detection to Intrusion Prevention.....	29
Geo Protection/Policy & Updatable Geo Objects.....	31
Anti-Virus Protection.....	33
Post-Infection Detection: Anti-Bot.....	36
Enabling the IPS/AV/ABOT Features for the First Time.....	38
Lab Exercise: Explore the Training Lab Environment.....	40
Lab Tips.....	42
Module 2 – Working With IPS Protections.....	47
IPS Protection Action.....	49
IPS Protection Tracking.....	51
Protection Attributes.....	53
Protection Ratings.....	54
Protection Ratings: Performance Impact.....	55
Protection Ratings: Severity.....	57
Protection Ratings: Confidence Level.....	59
The Four “Classes” of IPS Protections.....	61

IPS ThreatCloud Protections.....	63
IPS Core Activations.....	65
Inspection Settings.....	67
Which Policy Type Should I Install After Making a Change?.....	68
Sorting and Working with Protections.....	69
Protection Viewer – Hidden Columns.....	71
Protections Filters Tab.....	73
Protections Filters Tab +.....	75
Protections Search.....	76
Protections Handling – Bulk Operations.....	78
Lab Exercise: Configuring IPS Protections.....	80
Working with Inspection Settings.....	80
Working with IPS ThreatCloud Protections.....	81
Working with Core Activations.....	87
Module 3 – Working with AV/ABOT Protections.....	89
The Anti-Virus Blade.....	89
Supported Network Protocols.....	90
Anti-Virus Deep & Archive Scanning – What Are They?.....	91
The Anti-Bot Blade.....	94
Anti-Virus and Anti-Bot Protection Types.....	95
Viruses.....	96
Reputation IPs, URLs & Domains.....	96
URLs with Malware.....	96
Unusual Activity & Malicious Activity.....	96
File Types.....	97
Mail Activity & Links Inside Mail.....	97
Email Scanning: To MTA or not to MTA.....	97
The Malware DNS Trap.....	98
General Anti-Virus/Anti-Bot Settings.....	100
Fail Mode: Fail-open vs. Fail-closed.....	101
Background (Rapid Delivery) vs. Hold (Maximum Prevention).....	101

Lab Exercise: Working with Anti-Virus and Anti-Bot Protections.....	104
Module 4 – Threat Prevention Profiles & Policy Layers.....	110
Threat Prevention (TP) Profile Basics.....	111
Default Profiles: Optimized vs. Strict vs. Basic.....	112
TP Profiles Comparison.....	114
Profile General Policy.....	116
Profile Settings for IPS ThreatCloud Protections.....	117
Profile Settings for IPS Core Activations.....	119
Profile Settings for Anti-Virus.....	120
Anti-Virus Traffic Direction and Interface Type Settings.....	121
Profile Settings for Anti-Bot.....	122
TP Profile Best Practices.....	123
Cloning Profiles.....	123
New TP Profile Workflow.....	124
The Threat Prevention Policy Layers.....	126
New TP Policy Layer Rule Workflow.....	126
The Legacy "IPS" Threat Prevention Layer.....	128
Notifying/Challenging the User: UserChecks.....	129
TP Policy Actions: Block vs. Prevent vs. Detect vs. Inactive vs. Redirect.....	131
How Profiles are Matched in the TP policy.....	132
Matching when Multiple TP Policy Layers are Present.....	133
TP Policy Best Practices.....	135
Miscellaneous: IPS Profile Cleanups.....	136
Miscellaneous: Protected Servers Checkboxes.....	138
Lab Exercise: Assigning TP Profiles to a TP policy.....	139
Enabling the IPS Blade.....	139
Cloning & Customizing IPS Profiles.....	139
Working with Threat Prevention Policies.....	141
Module 5 – Updatable Geo Objects & Geo Protection/Policy.....	143
The Need to Enforce Geographic Policies.....	143

Really Old School: "Geo Protection" in R77.30.....	144
Old School: Geo Policy in R80+.....	145
Geo Policy Profiles.....	147
Geo Policy Activation Mode.....	149
Geo Policy for Specific Countries.....	151
Geo Policy Tips & Tricks.....	153
New School: Geo Updatable Objects (R80.20+).....	155
Geo Updatable Objects Tips & Tricks.....	157
Geo Policy Troubleshooting Case Study.....	159
Lab Exercise: Work with the Legacy Geo Policy; Deploy Geo Objects & Test.....	160
Cloning and Customizing a Geo Policy.....	160
Testing Geo Policy Enforcement.....	163
Utilizing Geo Updatable Objects.....	164
Testing Geo Updatable Objects Enforcement.....	166
Module 6 – HTTPS Inspection.....	167
HTTPS Inspection...Why do we need it?.....	167
Full Outbound HTTPS Inspection.....	168
The Full Outbound Certificate Forging Game.....	168
Quick Mention: Outbound "Lite" Inspection a.k.a. Categorize HTTPS Sites.....	169
Quick Mention: Inbound HTTPS Inspection.....	171
The HTTPS Inspection Policy.....	172
Tips for Configuring the HTTPS Policy & Best Practices.....	173
HTTPS Inspection & Proxies.....	178
Additional HTTPS Inspection Settings.....	179
HTTPS Inspection Troubleshooting.....	182
SSL Inspection over RDP.....	184
SSH Deep Packet Inspection.....	185
ICAP Integration.....	185
Mirror & Decrypt a.k.a. Decrypt and Forward.....	186
Lab Exercise: Configuring & Testing HTTPS Inspection.....	188

Visit Test Virus and Malware Sites.....	188
Visit Test Virus and Malware Sites in Prevent Mode.....	189
Enable Full Outbound HTTPS Inspection & Create a HTTPS Inspection Policy.....	190
Test HTTPS Inspection.....	195
Create a Custom Site Bypass.....	199
<b>Module 7 – Log Analysis, Packet Captures &amp; Creating Exceptions/Exclusions.....</b>	<b>201</b>
TP Policy Tracking Options: Log, Packet Captures, & Advanced Forensics.....	202
The Check Point ThreatWiki.....	203
Example IPS Log.....	205
Example Anti-Virus Log.....	207
Example Anti-Bot Log.....	208
Log Filtering Syntax.....	210
Undocking Log Tabs.....	212
Viewing Logs by Threat Prevention Rule.....	214
Using Browser-based SmartView to View Logs.....	215
Session Logging.....	216
Log Suppression.....	220
Exceptions: Inspection Settings/IPS/Geo Policy.....	222
Inspection Settings Exceptions.....	223
IPS ThreatCloud/Anti-Virus/Anti-Bot Exceptions.....	225
Core Activations Exceptions.....	227
Geo Policy Exceptions (Legacy).....	229
Exception Creation Shortcut Method 1 – Log Card.....	231
Exception Creation Shortcut Method 2 – Log Overview.....	232
Exceptions Tips & Tricks.....	233
IPS Implied Exceptions.....	234
Anti-Virus Allow List & Anti-Bot Email Exclusions.....	235
Case Study: Missing Logged Protections.....	237
<b>Lab Exercise: Simulate Attacks, Investigate with Logs &amp; Create Exceptions.....</b>	<b>239</b>
Launch Attacks, Observe Log Suppression, and Create a ThreatCloud Protection Exception.....	239

Viewing IPS Packet Captures.....	241
Create an Inspection Settings Exception.....	243
Create a Core Activations Exception.....	245
Use the SmartView Web Interface to View Logs.....	247
<b>Module 8 – Threat Prevention Correlated Views &amp; Reports.....</b>	<b>248</b>
The Need for SmartEvent.....	248
Defining the Internal Network in SmartEvent.....	249
SmartEvent Threat Prevention Views.....	252
SmartEvent Threat Prevention Reports.....	256
Most Useful TP Views and Reports in the Real World.....	258
TP Views/Reports Customization and Tips & Tricks.....	262
Threat Prevention Investigative Best Practices.....	267
Beyond SmartEvent – Check Point Infinity SOC.....	268
Exporting Logs to a SIEM for External Reporting.....	268
<b>Lab Exercise: Examining IPS/AV/ABOT Views &amp; Reports.....</b>	<b>270</b>
Verify Activation of SmartEvent on the SMS.....	270
Generate Additional Logs for Reporting.....	272
Work with SmartEvent Views and Reports.....	273
<b>Module 9 – IPS/AV/ABOT Updates.....</b>	<b>276</b>
When Did the Last Update Occur?.....	276
IPS Updates.....	277
Staging/Detect Only Modes & Follow Up.....	282
Anti-Virus/Anti-Bot Updates: Not Just a Downloaded Patterns File.....	289
Offline Updates.....	290
IPS Update Failures Troubleshooting.....	291
Rolling Back Bad Updates/Forcing an Update.....	292
Update Failures on the Standby ClusterXL Member.....	298
How to Report False Positives to Check Point.....	298
TP License Expiration Ramifications.....	299
<b>Lab Exercise: Verifying Recent Updates &amp; Setting Detect Only Mode.....</b>	<b>300</b>

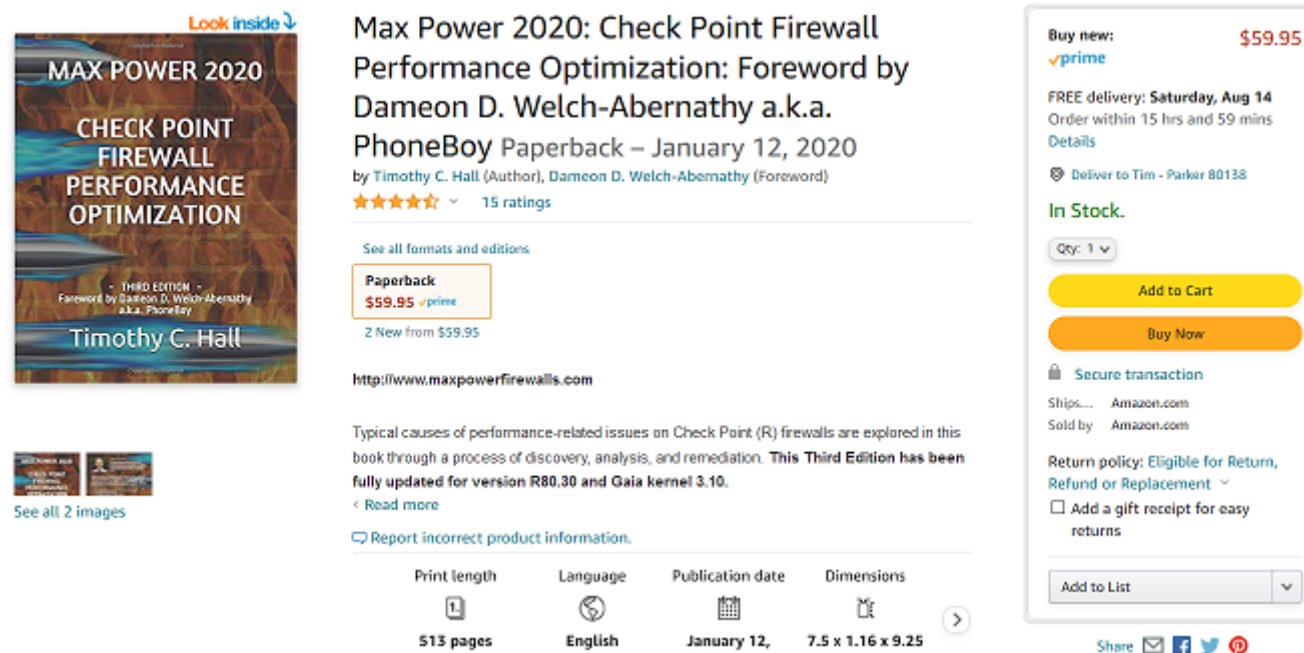
Module 10 – Threat Prevention Monitoring & Alerts.....	304
SNMP Monitoring.....	308
SNMP Get Capabilities.....	311
Receiving Basic SNMP Traps and/or Email Alerts.....	312
Basic Alert Destinations.....	316
Advanced Alerting.....	318
User-defined Alerts.....	318
SmartEvent Automatic Reactions.....	319
Case Study: Alert for All IPS Events, But Only for a Certain IP Address.....	323
Receiving Check Point Threat Intelligence Email Updates.....	324
Lab Exercise: Configure and Test SNMP, SNMP Traps, and SmartEvent Automatic Reactions.....	325
Walk the SNMP Tree.....	325
Configure a Simple SNMP Trap.....	328
Configure a SmartEvent Automatic Reaction.....	330
Module 11 – Advanced IPS/AV/ABOT Features & Troubleshooting Techniques.....	333
Adding Custom SNORT Protections (Signatures).....	333
Automated Custom Intelligence Feeds & Custom Threat Indicators.....	336
How to Create Test IPS/AV/ABOT Traffic.....	337
Order of Enforcement by the Firewall.....	339
Auditing Changes Made to the TP Configuration.....	340
CLI Check: Verify the Active Member in ClusterXL!!!.....	342
How to View all Traffic being Denied by the Firewall in Real-Time, and Why.....	344
How to Disable IPS & Anti-Virus/Anti-Bot Instantly on a Firewall.....	346
IPS on Gaia Embedded Appliances.....	347
Lab Exercise: Add Custom Protections, View Real-time Drops, and Audit Configuration Changes.....	348
Create & Test a Custom Threat Indicator.....	351
Observe Firewall Drops in Real Time.....	352
Auditing Configuration Changes.....	354
Module 12 – Threat Prevention Performance Optimization.....	358
SecureXL.....	358



CoreXL.....	359
The Four Paths.....	360
TP Performance Optimization: Performance Tuning.....	361
Don't Do It: IPS Bypass Under Load.....	362
Threat Prevention Optimization: The "Null Profile" Trick.....	363
HTTPS Inspection Policy Optimization.....	365
Dealing with a SYN Attack (SYN Flood).....	366
DoS Response Tactics: The SecureXL Penalty Box.....	366
Using the IPS Collector On-demand Troubleshooting Tool.....	368
Lab Exercise: The SecureXL Penalty Box, Null Profiles, and Stopping All TP Enforcement Instantly (Optional)....	369
Create a Null Profile.....	371
The Panic Button: Stopping all Threat Prevention Enforcement Instantly.....	373
Module 13: R81.10 Preview: Autonomous Threat Prevention Management & MITRE ATT&CK Reports.....	375
R81 and R81.10: What's new with IPS/AV/ABOT & HTTPS Inspection.....	375
The Need for Autonomous Threat Prevention Management.....	375
MITRE ATT&CK Reporting.....	379
Live Demo: Deploy Autonomous Threat Prevention Management in R81.10 & View MITRE ATT&CK Reports....	381
Wrap-up Discussion and Additional Resources.....	382

# Welcome & Introduction

- Your Instructor: **Timothy Hall, CISSP**
  - Worked with Check Point products since 1997, Check Point instructor since 2004
  - Founder of Shadow Peak Inc, a Check Point Authorized Training Center (ATC) (<http://www.shadowpeak.com>)
  - [Link to all CheckMates Posts](#) and [Link to all CPUG Posts](#)
  - Creator of the self-guided video training series "Check Point IPS Immersion", "Gaia 3.10 Immersion" and "Max Capture: Know Your Packets"
  - Author of Book “Max Power 2020: Check Point Firewall Performance Optimization”



**MAX POWER 2020**  
**CHECK POINT**  
**FIREWALL**  
**PERFORMANCE**  
**OPTIMIZATION**  
- THIRD EDITION -  
Foreword by Dameon D. Welch-Abernathy  
a.k.a. PhoneBoy  
Timothy C. Hall

**Max Power 2020: Check Point Firewall Performance Optimization: Foreword by Dameon D. Welch-Abernathy a.k.a. PhoneBoy** Paperback – January 12, 2020  
by Timothy C. Hall (Author), Dameon D. Welch-Abernathy (Foreword)  
★★★★★ 15 ratings

See all formats and editions

**Paperback**  
**\$59.95** ✓prime  
2 New from \$59.95

<http://www.maxpowerfirewalls.com>

Typical causes of performance-related issues on Check Point (R) firewalls are explored in this book through a process of discovery, analysis, and remediation. **This Third Edition has been fully updated for version R80.30 and Gaia kernel 3.10.**  
< Read more

Report incorrect product information.

Print length	Language	Publication date	Dimensions
513 pages	English	January 12,	7.5 x 1.16 x 9.25

Buy new: **\$59.95**  
✓prime  
FREE delivery: **Saturday, Aug 14**  
Order within 15 hrs and 59 mins  
Details  
Deliver to Tim - Parker 80138  
**In Stock.**  
Qty: 1  
**Add to Cart**  
**Buy Now**  
Secure transaction  
Ships from Amazon.com  
Sold by Amazon.com  
Return policy: Eligible for Return, Refund or Replacement  
 Add a gift receipt for easy returns  
Add to List

Share

## Check Point IPS/AV/ABOT Immersion Class Details

- Prerequisites: Basic systems and networking knowledge.
- We will be working with the R80.40 Check Point code, however the final module will provide a preview of the new Threat Prevention configuration automation operations in version R81.10
- The main focus of this course is the R80.40 code running on Check Point appliances (models 2200-28XXX), open hardware, and some types of virtualized environments.
- The material presented in this course will also apply to CloudGuard gateways subject to the specific limitations detailed in [sk160753: Check Point R80.40 Known Limitations](#) and to a lesser degree Section 7 of this SK: [sk141173: Check Point R80.20 with Gaia 3.10 for CloudGuard and Open Server Security Gateways](#).
- Hyperlinks shown in this document are “hot” and can be clicked to show the specified resource in your web browser.

## List of Class Modules

- Module 0 – Crash Course: The Basics of Check Point Objects, Policies & Logging (optional)
- Module 1 – History of IDS/SmartDefense/IPS/AV/ABOT
- Module 2 – Working with IPS Protections
- Module 3 – Working with AV/ABOT Protections
- Module 4 – Threat Prevention Profiles & Policy Layers
- Module 5 – Updatable Geo Objects & Geo Protection/Policy
- Module 6 – HTTPS Inspection
- Module 7 – Log Analysis, Packet Captures & Creating Exceptions/Exclusions
- Module 8 – Threat Prevention Correlated Views & Reports
- Module 9 – IPS/AV/ABOT Updates
- Module 10 – Threat Prevention Alerts & Monitoring
- Module 11 – Advanced IPS/AV/ABOT Features & Troubleshooting Techniques
- Module 12 – Threat Prevention Performance Optimization
- Module 13 – R81.10 Preview: Autonomous Threat Prevention Management