

Check Point IPS/AV/ABOT Immersion R81.20 Update



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.....	35
Enabling the IPS/AV/ABOT Features for the First Time – Custom TP.....	37
Initial Lab Exercise.....	40
Lab Access Tips.....	42
Explore the Training Lab Environment.....	43
Module 2 – Working With IPS Protections.....	48
IPS Protection Action.....	50
IPS Protection Tracking.....	52
Protection Attributes.....	54
Protection Ratings Overview.....	55
Protection Ratings: Performance Impact.....	56

Protection Ratings: Severity.....	58
Protection Ratings: Confidence Level.....	60
The Four “Classes” of IPS Protections.....	62
Class #1: IPS ThreatCloud Protections.....	64
Class #2: IPS Core Activations.....	66
Class #3: Inspection Settings.....	68
Class #4: Geo Policy (deprecated).....	70
Which Policy Type Should I Install After Making a Change?.....	70
Sorting and Working with Protections.....	71
Protection Viewer – Hidden Columns.....	73
Protections Filters Tab.....	75
Protections Filters Tab +.....	77
Protections Search.....	78
Protections Handling – Bulk Operations.....	80
Lab Exercise: Configuring IPS Protections.....	82
Working with Inspection Settings.....	82
Working with IPS ThreatCloud Protections.....	83
Working with Core Activations.....	89
Module 3 – Working with AV/ABOT Protections.....	91
The Anti-Virus Blade.....	91
Supported Network Protocols.....	92
Anti-Virus Deep & Archive Scanning – What Are They?.....	93
The Anti-Bot Blade.....	96
Anti-Virus and Anti-Bot Protection Types.....	97
Viruses.....	98
Reputation IPs, URLs & Domains.....	98
URLs with Malware.....	98
Unusual Activity & Malicious Activity.....	98
File Types.....	99
Mail Activity & Links Inside Mail.....	99
Advanced File Inspection.....	99

R81.20 Additional "Under the Hood" DNS Protections in Anti-Bot.....	100
Email Scanning: To MTA or not to MTA.....	100
The Malware DNS Trap.....	101
General Anti-Virus/Anti-Bot Settings.....	103
Fail Mode: Fail-open vs. Fail-closed.....	104
Background (Rapid Delivery) vs. Hold (Maximum Prevention).....	105
Lab Exercise: Working with Anti-Virus and Anti-Bot Protections.....	108
Module 4 – Threat Prevention Profiles & Policy Layers.....	114
Threat Prevention (TP) Profile Basics.....	115
Default Profiles: Optimized vs. Strict vs. Basic.....	116
TP Profiles Comparison.....	117
Profile General Policy.....	119
Profile Settings for IPS ThreatCloud Protections & Additional Activation.....	120
Profile Settings for IPS Core Activations.....	122
Profile Settings for Anti-Virus.....	123
Anti-Virus Traffic Direction and Interface Type Settings.....	124
Profile Settings for Anti-Bot.....	125
TP Profile Best Practices.....	126
Cloning Profiles.....	126
New TP Profile Workflow.....	127
The Threat Prevention Policy Layers.....	131
New TP Policy Layer Rule Workflow.....	131
The Legacy "IPS" Threat Prevention Layer.....	133
Notifying/Challenging the User: UserChecks.....	135
TP Policy Actions: Block vs. Prevent vs. Detect vs. Inactive vs. Redirect.....	137
How Profiles are Matched in the TP policy.....	138
Matching when Multiple TP Policy Layers are Present.....	139
TP Policy Best Practices.....	141
Miscellaneous: IPS Profile Cleanups.....	142
Miscellaneous: Protected Servers Checkboxes.....	144
Lab Exercise: Assigning TP Profiles to a TP policy.....	145

Enabling the IPS Blade.....	145
Cloning & Customizing IPS Profiles.....	145
Working with Threat Prevention Policies.....	148
Module 5 – Updatable Geo Objects & Geo Protection/Policy.....	151
The Need to Enforce Geographic Policies.....	151
Really Old School: "Geo Protection" in R77.30.....	152
Old School: Geo Policy in R80+.....	153
Geo Policy Profiles.....	155
Geo Policy Activation Mode.....	157
Geo Policy for Specific Countries.....	159
Geo Policy Tips & Tricks.....	161
New School: Geo Updatable Objects (R80.20+).....	163
Geo Updatable Objects Tips & Tricks.....	166
Geo Policy Troubleshooting Case Study.....	169
Lab Exercise: Work with the Legacy Geo Policy; Deploy Geo Objects & Test.....	170
Cloning and Customizing a Geo Policy.....	170
Testing Geo Policy Enforcement.....	173
Utilizing Geo Updatable Objects.....	174
Testing Geo Updatable Objects Enforcement.....	176
Module 6 – HTTPS Inspection.....	177
HTTPS Inspection...Why do we need it?.....	177
Full Outbound HTTPS Inspection.....	178
The Full Outbound Certificate Forging Game.....	179
Quick Mention: Outbound "Lite" Inspection a.k.a. Categorize HTTPS Sites.....	180
Quick Mention: Inbound HTTPS Inspection.....	181
The HTTPS Inspection Policy.....	182
Tips for Configuring the HTTPS Inspection Policy & Best Practices.....	184
HTTPS Inspection & Proxies.....	189
Additional HTTPS Inspection Settings.....	190
HTTPS Inspection Troubleshooting.....	193

SSH Deep Packet Inspection.....	197
ICAP Integration.....	198
Mirror & Decrypt a.k.a. Decrypt and Forward.....	199
Lab Exercise: Configuring & Testing HTTPS Inspection.....	201
Visit Test Virus and Malware Sites.....	201
Visit Test Virus and Malware Sites in Prevent Mode.....	202
Enable Full Outbound HTTPS Inspection & Create a HTTPS Inspection Policy.....	204
Test HTTPS Inspection.....	209
Module 7 – Log Analysis, Packet Captures & Creating Exceptions/Exclusions.....	214
TP Policy Tracking Options: Log, Packet Captures, & Advanced Forensics.....	215
The Check Point ThreatWiki.....	217
Example IPS Log.....	219
Example Anti-Virus Log.....	221
Example Anti-Bot Log.....	222
Log Filtering Syntax.....	224
Undocking Log Tabs.....	226
Viewing Logs by Threat Prevention Rule.....	228
Using Browser-based SmartConsole to View Logs.....	229
Session Logging.....	230
Log Suppression.....	234
Exceptions: Inspection Settings/IPS/Geo Policy.....	236
Inspection Settings Exceptions.....	238
IPS ThreatCloud/Anti-Virus/Anti-Bot Exceptions.....	240
Core Activations Exceptions.....	241
Geo Policy Exceptions (Legacy).....	243
Exception Creation Shortcut Method 1 – Log Card.....	245
Exception Creation Shortcut Method 2 – Log Overview.....	246
Exceptions Tips & Tricks.....	247
IPS Implied Exceptions.....	248
Anti-Virus Allow List & Anti-Bot Email Exclusions.....	249

Case Study: Missing Logged Protections.....	251
Lab Exercise: Simulate Attacks, Investigate with Logs & Create Exceptions.....	253
Launch Attacks, Observe Log Suppression, and Create a ThreatCloud Protection Exception.....	253
Viewing IPS Packet Captures.....	255
Create an Inspection Settings Exception.....	257
Create a Core Activations Exception.....	259
Use the SmartConsole Web Interface to View Logs.....	261
Module 8 – Threat Prevention Correlated Views & Reports.....	262
The Need for SmartEvent.....	262
Defining the Internal Network in SmartEvent.....	263
SmartEvent Threat Prevention Views.....	266
MITRE ATT&CK Reporting.....	270
SmartEvent Threat Prevention Reports.....	272
Most Useful TP Views and Reports in the Real World.....	274
TP Views/Reports Customization and Tips & Tricks.....	279
Threat Prevention Investigative Best Practices.....	284
Beyond SmartEvent – Check Point Infinity SOC & PRO Monitoring Service.....	285
Exporting Logs to a SIEM for External Reporting.....	285
Lab Exercise: Examining IPS/AV/ABOT Views & Reports.....	288
Verify Activation of SmartEvent on the SMS.....	288
Generate Additional Logs for Reporting.....	290
Work with SmartEvent Views and Reports.....	291
Module 9 – IPS/AV/ABOT Updates.....	294
When Did the Last Update Occur?.....	294
IPS Updates.....	295
Anti-Virus & Anti-Bot "Updates".....	299
Staging/Detect Only Modes & Follow Up.....	300
Anti-Virus/Anti-Bot Updates: Not Just a Downloaded Patterns File.....	307
Offline Updates.....	308
IPS Update Failures Troubleshooting.....	309

Rolling Back Bad Updates/Forcing an Update.....	310
Update Failures on the Standby ClusterXL Member.....	316
How to Report False Positives to Check Point.....	316
ThreatCloud Intelligence Sharing Settings.....	317
TP License Expiration Ramifications.....	318
Lab Exercise: Verifying Recent Updates & Setting Detect Only Mode.....	319
Module 10 – Threat Prevention Monitoring & Alerts.....	323
SNMP Monitoring.....	327
SNMP Get Capabilities.....	330
Receiving Basic SNMP Traps and/or Email Alerts.....	331
Basic Alert Destinations.....	335
Advanced Alerting Capabilities.....	336
User-defined Alerts.....	337
SmartEvent Automatic Reactions.....	338
Case Study: Alert for All IPS Events, But Only for a Certain IP Address.....	342
Receiving Check Point Threat Intelligence Email Updates.....	343
New Monitoring Frontiers – Skyline.....	343
Lab Exercise: Configure and Test SNMP, SNMP Traps, and SmartEvent Automatic Reactions.....	345
Walk the SNMP Tree.....	345
Configure a Simple SNMP Trap.....	348
Configure a SmartEvent Automatic Reaction.....	350
Module 11 – Advanced IPS/AV/ABOT Features & Troubleshooting Techniques.....	353
Adding Custom SNORT Protections (Signatures).....	353
Automated Custom Intelligence Feeds & Custom Threat Indicators.....	357
How to Create Test IPS/AV/ABOT Traffic.....	359
Order of Enforcement by the Firewall.....	361
Auditing Changes Made to the TP Configuration.....	362
CLI Check: Verify the Active Member in ClusterXL!!!.....	366
How to View all Traffic being Denied by the Firewall in Real-Time, and Why.....	368
Last Resort Threat Prevention Troubleshooting Tool: tp_collector.....	370

Advanced Threat Prevention Configuration Options: The "malware_config" File.....	371
How to Disable IPS & Anti-Virus/Anti-Bot Instantly on a Firewall.....	372
Lab Exercise: Add Custom Protections, View Real-time Drops, and Audit Configuration Changes.....	374
Add Custom SNORT Rule (Optional – this will take 20+ minutes).....	374
Create & Test a Custom Threat Indicator.....	377
Observe Firewall Drops in Real Time.....	379
Auditing Configuration Changes & Changes Reports.....	381
Module 12 – Threat Prevention Performance Optimization.....	386
SecureXL.....	386
CoreXL.....	387
The Four Paths.....	388
TP Performance Optimization: Performance Tuning.....	389
Don't Do It: IPS Bypass Under Load.....	394
Threat Prevention Optimization: Blade-based Exceptions.....	396
Threat Prevention Blade-Based Exception Setup.....	397
Threat Prevention Optimization: The “Null Profile” Trick.....	401
HTTPS Inspection Policy Optimization.....	403
Dealing with a SYN Attack (SYN Flood).....	404
DoS Response Tactics: The SecureXL Penalty Box.....	404
Lab Exercise: The SecureXL Penalty Box, Null Profiles, and Stopping All TP Enforcement Instantly.....	406
Run "Secret" hcp Threat Prevention Performance Reports.....	406
Create a Null Profile.....	409
The Panic Button: Stopping all Threat Prevention Enforcement Instantly.....	411
Module 13: Autonomous Threat Prevention.....	413
Autonomous Threat Prevention – Requirements.....	416
Autonomous Threat Prevention – Tips, Tricks & Recommendations.....	417
Lab Exercise: Configure and Test Autonomous Threat Prevention.....	419
Wrap-up Discussion and Additional Resources.....	421

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 and exclusive instructor for the [R81.20 Gateway Performance Optimization class](#)
 - Also creator of the self-guided video training series "Gaia 3.10 Immersion" and "Max Capture: Know Your Packets"
 - Author of Book "Max Power 2020: Check Point Firewall Performance Optimization"

Check Point IPS/AV/ABOT Immersion Class Details

- Prerequisites: Basic systems and networking knowledge.
- We will be working with the R81.20, Jumbo HFA 8 Check Point code.
- The main focus of this course is the R81.20 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 [sk170418: Check Point R81.10 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.
- *Please note that this material can be taught by Mr. Hall as a live, 3-day class complete with real lab exercises for a minimum of 5 attendees. Contact sales@shadowpeak.com for more information.*

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 Monitoring & Alerts
- Module 11 – Advanced IPS/AV/ABOT Features & Troubleshooting Techniques
- Module 12 – Threat Prevention Performance Optimization
- Module 13 – Autonomous Threat Prevention