

# Check Point IPS Immersion Training



**Shadow Peak**

*SECURITY TRAINING AND SERVICES*

# Table of Contents

Module 0 – Welcome & Introduction.....	6
Check Point IPS Immersion Training Details.....	7
List of Class Modules.....	8
Module 1 – History of IDS/SmartDefense/IPS.....	9
IPS R77.XX -> R80.10.....	10
Lab 1: Explore the Training Lab Environment.....	11
Module 2 – The Basics: IPS Protections.....	14
IPS Protection Action.....	16
IPS Protection Tracking.....	18
Protection Attributes.....	20
Protection Ratings.....	22
Protection Ratings: Performance Impact.....	24
Protection Ratings: Severity.....	26
Protection Ratings: Confidence Level.....	28
The Four “Classes” of IPS Protections.....	30
IPS ThreatCloud Protections.....	32
IPS Core Activations.....	34
Inspection Settings.....	36
Which Policy Type Should I Install After Making a Change?.....	37
Sorting and Working with Protections.....	38
Protection Viewer – Hidden Columns.....	40
Protections Filters Tab.....	42
Protections Filters Tab +.....	44
Protections Search.....	46
Protections Handling Additional Tips.....	48
Lab 2: Configuring IPS Protections.....	50
Working with Inspection Settings.....	50
Working with IPS ThreatCloud Protections.....	51
Working with Core Activations.....	56
Module 3 – The Basics: IPS Profiles & Threat Prevention Layers.....	57
Default IPS Profiles.....	59

IPS Profile Comparison.....	61
IPS Profile Best Practices.....	63
Special Case: IPS Profiles and Gaia Embedded Appliances (1200R–1400).....	66
Additional IPS Protection Activation Using Tags.....	67
New IPS Profile Workflow.....	69
New TP Policy Layer Rule – R80.10+ Gateway.....	70
New TP Policy Layer Rule – R77.XX Gateway.....	72
R77.30 vs. R80.10 Management of IPS.....	76
Note: Protected Servers.....	77
Lab 3: Creating and Assigning IPS Profiles.....	79
Enabling the IPS Blade.....	79
Cloning & Customizing IPS Profiles.....	80
Working with Threat Prevention Policies.....	82
Module 4 – IPS Licensing & Geo Protection/Policy.....	84
Geo Protection – R77.XX.....	85
Geo Policy – R80.10.....	87
Geo Policy Profile.....	89
Geo Policy Activation Mode.....	91
Geo Policy for Specific Countries.....	93
Geo Policy Tips & Tricks 1.....	95
Geo Policy Tips & Tricks 2.....	97
Geo Policy Troubleshooting Case Study.....	98
Lab 4: Deploy Geo Policy.....	99
Cloning and Customizing a Geo Policy.....	99
Testing Geo Policy Enforcement.....	101
Module 5 – IPS Logging, Packet Captures & Creating Exceptions.....	103
Session Logging.....	103
IPS Log Suppression.....	107
IPS Log Filtering.....	109
Viewing Logs by Threat Prevention/IPS Rule.....	111
Undocking Log Tabs.....	112
Using Browser-based SmartView to View Logs.....	113

Full-time IPS Packet Captures.....	115
Packet Captures Tips & Tricks 1.....	117
Packet Captures Tips & Tricks 2.....	119
Exceptions: Geo Policy/Inspection Settings/IPS/TP.....	121
Geo Policy Exceptions.....	122
Inspection Settings Exceptions.....	124
ThreatCloud IPS Exceptions.....	126
Core Activations Exceptions.....	128
Exception Creation Shortcut Method 1 – Log Card.....	130
Exception Creation Shortcut Method 2 – Log Overview.....	131
Exceptions Tips & Tricks.....	132
IPS Implied Exceptions.....	133
Lab 5: Simulate Attacks, Investigate with Logs & Create Exceptions.....	135
Launch Attacks and Observe Log Suppression.....	135
Launch Attacks and Create ThreatCloud Protection Exceptions from Logs.....	136
Viewing IPS Packet Captures.....	138
Creating a Geo Policy Exception.....	141
Create an Inspection Settings Exception.....	142
Use the SmartView Web Interface to View IPS Logs.....	142
Module 6 – IPS Views & Reports.....	144
IPS Views Customization.....	146
IPS Views Tips & Tricks.....	148
IPS Reports.....	150
IPS Reports Tips & Tricks.....	152
Lab 6: Examining IPS Views & Reports.....	154
Module 7 – IPS Updates & Staging/Detect Mode.....	155
IPS Update Failures Troubleshooting.....	157
Backing Out IPS Updates.....	158
Working with Protections in Staging Mode.....	162
Lab 7: IPS Updates & Staging Mode.....	167
Module 8 – R80.20 IPS Preview.....	170
R80.20 IPS – Automatic Gateway IPS Updates.....	171

R80.20 Use of Geo Countries in Main Policy Layers.....	172
R80.20 IPS - Now Reports as a Separate Blade.....	173
R80.20 IPS – Staging, Follow Up and Comments.....	174
R80.20 IPS – Miscellaneous Topics.....	176
Lab 8: R80.20 Live Demo.....	177
Module 9 – Advanced IPS Troubleshooting & Tips.....	178
IPS on Gaia Embedded Appliances.....	178
Management Command Line for IPS/TP.....	179
Auditing Changes Made to the IPS Configuration.....	181
Miscellaneous IPS Features & Troubleshooting.....	183
Lab 9: Explore the Management CLI & Audit IPS Changes.....	184
Module 10 – IPS Performance Optimization.....	186
SecureXL.....	186
CoreXL.....	187
The Three Paths: R80.10 and Earlier.....	188
IPS Performance Optimization: Performance Tuning.....	189
IPS Optimization: The “Null Profile” Trick.....	190
IPS Bypass Under Load.....	192
Measuring IPS Performance Impact & Impact of Top Protections.....	194
Special Case: Optimizing IPS with Gaia Embedded Appliances.....	195
Wrap–up Discussion and Additional Resources.....	196

# Module 0 – Welcome & Introduction

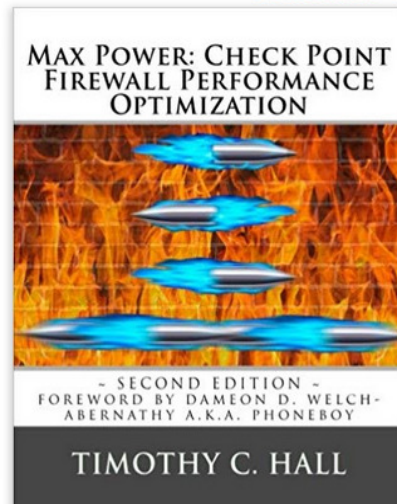
- Your Instructor: **Timothy Hall, CISSP**
  - Additional Certifications: CCSI, CCSM, CCNA Security
  - Worked with Check Point products since 1997, Check Point instructor since 2004
  - Founder of Shadow Peak Inc, a Check Point Authorized Training Center (ATC) (<http://www.shadowpeak.com>)
  - [Link to all CheckMates Posts](#)
  - [Link to all CPUG Posts](#)
  - Author of Book “Max Power: Check Point Firewall Performance Optimization”

## Max Power: Check Point Firewall Performance Optimization Second Edition

by [Timothy C Hall](#) (Author), [Dameon D. Welch-Abernathy](#) (Foreword)

★★★★★ 5 customer reviews

[Look inside](#)



**Paperback**  
\$59.95

**Other Sellers**  
from \$59.95

Buy new

✓prime \$59.95

FREE Delivery by **Wednesday**, or

1 New from \$59.95

Get it **Tuesday** if you order within 26 hrs 43 mins and choose paid shipping at checkout. [Details](#)

📍 Deliver to Tim - Parker 80138

**In Stock.**

Qty: 1

Ships from and sold by Amazon.com. Gift-wrap available.

✓prime

Add to Cart

Buy Now