



Gateway Performance Optimization

Timothy C. Hall, Shadow Peak Inc.



Table of Contents

Welcome & Introduction.....	10
Gateway Performance Optimization Class Details.....	11
List of Class Modules.....	12
Module 1 – R81.20 Performance Introduction & Concepts.....	13
Introduction.....	13
Background: Check Point™ History & Architecture.....	13
Your Best Friend: GA Jumbo Hotfix Accumulators.....	15
Useful Performance-Related CheckMates Community Tools.....	15
The “Super Seven” Performance Assessment Commands.....	16
“Super Seven” in the SmartConsole.....	17
Common Check Point™ Commands (ccc) by Danny Jung.....	18
CheckMates “One-Liners”	19
Gateway Performance Optimization Lab Tips.....	23
Beware: Speed Tests & Client-based AntiMalware/AntiVirus Software.....	26
Lab Exercise 1: Explore the Lab, Initial Speed Tests, & CheckMates Community Tools.....	27
Explore the Current Configuration in the SmartConsole.....	27
Execute Initial Speed Tests and Note Awful Performance.....	29
Work with ccc and s7pac “Super Seven”.....	31
Module 2 – Network Level Optimization.....	34
Background.....	34
Latency/Jitter vs. Loss.....	34
New Connection Rates & Rulebase Lookups.....	37
Measuring Firewall Latency & Application Performance.....	38
IP Fragments Effect on Performance.....	40
The RX “Dark Triad”	41
Network Interface Stability, Error Counters, & Interface Speed Checks.....	42
Mitigating Overruns (RX-OVR): Interface Bonding.....	43
A Common Issue: Bond Traffic Imbalances!.....	43
A Controversial Option: Ethernet Flow Control/Pause Frames.....	44

Special Case: RX-OVR and RX-DRP Increment in "Lockstep".....	44
Other Network Interface Errors: RX-ERR.....	45
Clearing Network Counters.....	45
What about RX-DRP?.....	45
Network Driver Updates – Look Out!.....	45
ARP Neighbor Table Overflows.....	47
Lab Exercise 2: Diagnose & Correct Network Performance Issues.....	49
Execute Failover and Run Speed Tests Again.....	49
Fail back Over and Troubleshoot High Latency.....	50
Measure Firewall Latency & Continue Troubleshooting.....	51
Troubleshoot Bandwidth Issues.....	52
Troubleshoot Packet Loss.....	53
Check Firewall Network Counters.....	53
Correct External Network Issues.....	54
Module 3 – Basic Gaia 3.10/RHEL Optimization.....	60
Background.....	60
Gaia Kernel Updates.....	60
Introduction: User Space Firewall (USFW).....	61
The “top” & “free” Gaia/Linux Commands.....	64
Top Output: “us” & “ni” – Process/User Space.....	65
Top Output: “sy” & ”si” – System Space.....	66
Top Output: “wa” – Waiting for I/O Operation.....	66
Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles.....	67
CPU Usage Spikes: Introducing the Spike Detective.....	68
Gaia Memory Management.....	69
Check Point™ Specific Commands.....	71
Memory Allocation Failures.....	71
Connection Table Overflows.....	72
Special Case: Maestro & Connection Table Overflows.....	77
HealthCheck Point™ (HCP).....	78
Lab Exercise 3: Examine Gaia Health & Optimize.....	80

Run HealthCheck Point™.....	80
Run healthcheck.sh.....	82
Unlock & Run "Secret" hcp Performance Reports.....	82
Launch Policy Installation and Observe Waiting for I/O.....	84
Resolve Memory Shortages.....	87
Run Speed Tests and Observe Core Utilization.....	90
Launch Port Scan and Observe Connection Table Behavior.....	90
Module 4 – ClusterXL Performance Tuning.....	94
A Quick Note: SDF and the Correction Layer.....	94
Sync Network Health Check.....	94
Selective Synchronization of Services & Delayed Sync.....	96
Verifying Proper Cluster Operation.....	99
One More Thing: The "Cluster Under Load" Mechanism.....	99
Lab Exercise 4: Verify Cluster Operation & Sync Network Health.....	100
Checking Cluster Status.....	100
Cause a Catastrophic Failover and Observe Behavior.....	100
Cause a Non-Catastrophic Failover and Observe Behavior.....	103
Check & Correct Sync Network Health.....	103
Verify the Default Setting for Delayed Sync.....	106
Module 5 – CoreXL & Multi-Queue.....	107
Old School <R81: CoreXL "Static Split".....	108
New School R81+: CoreXL Dynamic Balancing ("Dynamic Split").....	110
RX-DRP & Ring Buffer Sizes.....	114
Multi-Queue Introduction.....	116
Multi-Queue Parallel Queues Limitations.....	116
The Dynamic Dispatcher & Priority Queueing.....	118
SND/IRQ Core Balancing.....	121
Tracking Down Unexplained High CPU Usage: The Undocumented "perf" Command.....	123
Troubleshooting Persistent, Excessive CPU Utilization on a Particular Core.....	124
CoreXL Frontiers: Intel’s "P-Cores"/"E-Cores".....	127
Lab Exercise 5: Multi-Queue, CoreXL Splits, and Static CoreXL Split Changes.....	128
Examine Multi-Queue Configuration.....	128

Correct Multi-Queue & Ring Buffer Issues.....	129
Work with the Dynamic Dispatcher/Priority Queues & Enable.....	130
Modifying the Static CoreXL Split.....	133
Module 6 – SecureXL Throughput Acceleration.....	137
SecureXL Introduction Part 1 - Throughput Acceleration.....	137
SecureXL Introduction Part 2 – Accept Templates.....	138
Throughput Acceleration – fwaccel stats -s.....	140
Accelerated conns/Total conns (Software Accept Template Match).....	141
LightSpeed conns/Total Conns (Hardware Accept Template Match).....	141
Accelerated pkts/Total pkts (Software Fastpath).....	141
LightSpeed pkts/Total pkts (Hardware Fastpath).....	141
F2Fed pkts/Total pkts.....	141
F2V pkts/Total pkts.....	142
CPASXL pkts/Total pkts.....	142
PSLXL pkts/Total pkts.....	142
CPAS Pipeline & PSL Pipeline.....	143
UDP IS XL pkts/Total pkts & UDP IS pipeline pkts/Total pkts (R82+ only).....	143
QOS inbound & outbound pkts/Total pkts.....	143
Corrected pkts/Total pkts.....	143
Core Type Responsibilities & Relative Process Path Efficiency.....	143
Path Optimization Strategy.....	146
Corner Case: High Acceleration Rates & SMT/Hyperthreading.....	147
Selectively Disabling SecureXL.....	147
Forcing SecureXL Acceleration with fast_accel.....	149
The "fwaccel conns", "fw_mux all", fw_streaming, & "fw ctl multik gconn" Commands.....	152
Processing Path Determination Techniques.....	154
The Easy Way: "fw tab -t connections -z".....	154
The Hard Way: Performing a Kernel Debug.....	154
SecureXL Throughput Acceleration Limitations.....	155
SecureXL Frontiers: LightSpeed, UPPAK, & R82’s Parallel Processing Flows.....	157
Lab Exercise 6: Observing SecureXL Behavior & Determining Why Traffic is F2F.....	160
Examine Throughput Acceleration Levels.....	160

Execute Debug to Determine Why Certain Traffic is F2F/slowpath.....	163
Remove Manual F2F Definition.....	165
Set Up & Test Fast_Accel.....	168
Module 7 – Access Control Policy Tuning.....	170
Background.....	170
The Importance of a Properly Defined Firewall Topology.....	170
The Special Policy Object “Internet” & APCL/URLF Rules.....	174
rad Daemon Scalability Issues w/ Large User Populations.....	177
Access Control Rules: Column-based Matching.....	178
Beware: Use of Domain Objects, and Wildcards in Custom Application/Site Objects.....	179
SecureXL Session Rate Acceleration (Accept Templates).....	182
The Few Services & Rulebase Conditions That Can Still Disable Accept Templating in R80.10+.....	184
But Wait, the Actual Accept Templating Rate is Always Zero?.....	185
Cause #1: Enabling More Blades Than Just "Firewall" in the Top/Parent Policy Layer.....	185
Cause #2: Use of "Protocol Signature" Option on Service Objects.....	187
Zero Accept Template Rate Diagnosis: fwaccel templates -R.....	189
SecureXL Drop Templates and the Penalty Box.....	190
NAT Policy Optimization.....	192
IPSec VPN Performance Tuning.....	195
VPNs: 3DES vs. AES & AES New Instructions (AES-NI) & GCM.....	195
VPNs: IPSec: Low MTUs & PMTUD.....	198
Lab Exercise 7: Object Internet, Accept Templates, Optimizing APCL/URLF Policies.....	201
APCL/URLF Policy Optimization.....	201
Optimize SecureXL Accept Templates.....	205
Configure & Test the SecureXL Penalty Box.....	209
VPN Optimization Exercise.....	212
Module 8 – Threat Prevention Policy Tuning.....	216
Introduction.....	216
Quickly Assessing IPS/Threat Prevention Performance Impact.....	216
IPS Inspection Coverage: TP Main Layer vs. Legacy “IPS” Layer.....	218
Cut to the Chase: hcp’s Secret TP Reports.....	219

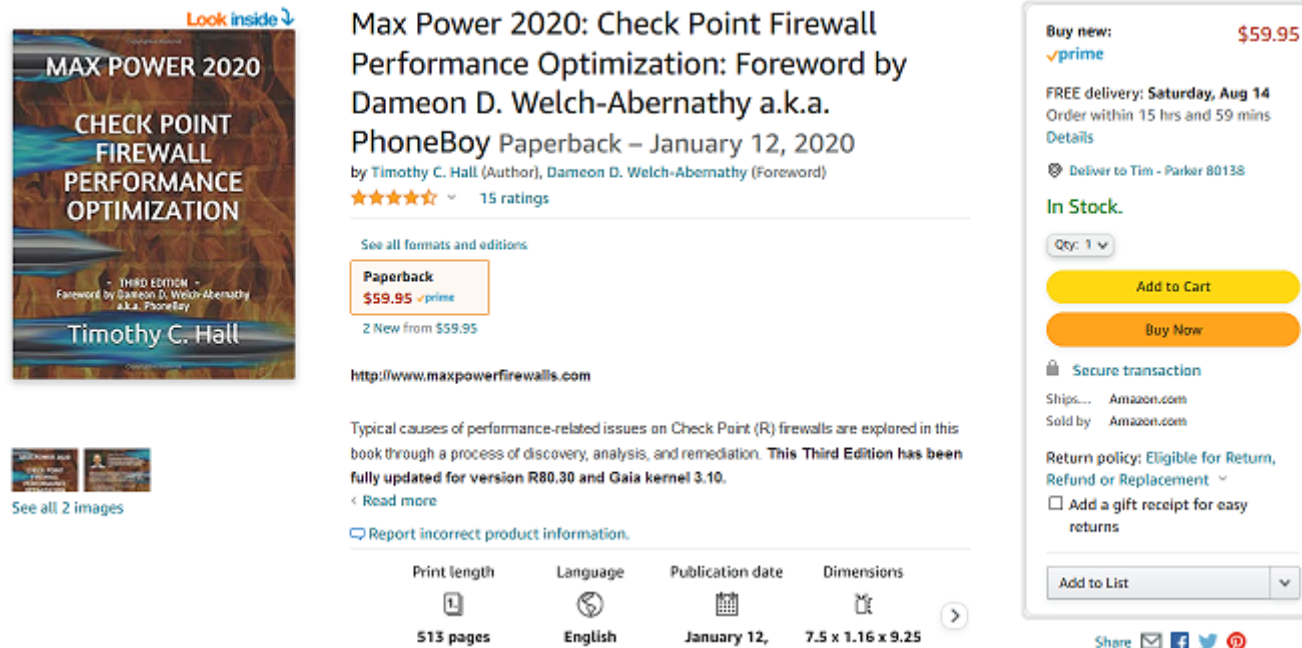
IPS Bypass Under Load: Formerly Unusable But Now an Option.....	222
Performance Impact: Inactive vs. Prevent vs. Detect.....	223
Custom IPS Profile Optimization: IPS ThreatCloud & Core Activations.....	223
Custom Profile Optimization: Inspection Settings.....	225
Performance: IPS Blade vs. Anti-Virus.....	226
Threat Prevention: “Null” Profiles vs. Blade-based Exceptions.....	230
Threat Prevention Blade-Based Exceptions.....	231
Threat Prevention "Null Profiles".....	234
Custom vs. Autonomous TP Policy Management.....	235
Lab Exercise 8: Finding F2F TP traffic, hcp, & Blade-based Exceptions.....	236
Diagnosing Threat Prevention Performance Issues.....	236
Disable Threat Prevention and Retest Performance.....	237
Run "Secret" hcp Threat Prevention Performance Reports.....	238
Examine SmartConsole Threat Prevention Configuration.....	241
Engage TP Profile Cleanup Options.....	242
Retest Performance after Optimizations.....	244
Create Blade-based Exception & Retest Speed.....	247
Module 9 – HTTPS Inspection Optimization.....	252
The Impact: Enabling HTTPS Inspection.....	252
Quick Mention: Outbound "Lite" Inspection a.k.a. Categorize HTTPS Sites.....	252
HTTPS Inspection Policy Optimization Best Practices.....	254
HTTPS Inspection Policy Tips & Tricks.....	256
HTTPS Inspection Frontiers in R82+.....	258
Lab Exercise 9: Optimize an HTTPS Inspection Policy (Optional).....	259
Identify Active Streaming Connections.....	259
Optimize Existing HTTPS Inspection Policy to Best Practices.....	261
Retest Active Streaming Performance After Optimizations.....	268
Verify HTTPS Inspection Policy Operation.....	270
Module 10 – Heavy Connections/Elephant Flows & HyperFlow/Pipeline Processing.....	272
Identifying Elephant/Heavy Connections.....	272

Remediating Elephant Flows.....	274
SecureXL Rate Limiting & Network Quotas.....	275
SecureXL and the Quality of Service (QoS) Blade.....	276
R81.20: HyperFlow & the "Pipeline" SecureXL Paths.....	276
HyperFlow Example.....	280
Monitoring/Configuring HyperFlow – CLI Commands.....	284
Monitoring HyperFlow – cpview.....	285
Monitoring HyperFlow – SmartConsole.....	288
Lab Exercise 10: Heavy Connections, Dynamic Split & HyperFlow.....	289
Create Multiple Elephant Flows & View Statistics.....	289
Enable Dynamic Balancing/Split & Hyperflow.....	291
Test Dynamic Split.....	292
Test HyperFlow/Pipeline Processing.....	296
Enforce Rate Limits.....	302
Appendix A – Intermittent/Historical Performance Issues Investigation & Monitoring.....	305
Syslog – A Frequently Effective Shortcut.....	305
cpview History Mode.....	306
Getting A “Second Opinion” - The sar Command.....	307
New Monitoring Frontiers – Skyline.....	311
Check the Spike Detective.....	313
What Else Changed?.....	313
SmartView Monitor Reports.....	314
Optional Lab: cpview History Mode & the sar Command.....	315
cpview Historical Mode.....	316
Getting a “Second Opinion” from the CLI with sar.....	316
Appendix B – Maestro/Scalable Platforms Commands.....	318
Live Performance Overview: asg perf -vp.....	318
Finding Performance "Hogs": asg_perf_hogs.....	320
Diagnostics for Scalable Platforms/Maestro: asg diag.....	321
Setting Limits with Session Control Rules: asg_session_control.....	322

Finding Which SGM (and path) is Handling a Degraded Connection: asg search.....	323
Packet Distribution Issues Between SGM's: show distribution.....	324
Appendix C: GEO Updatable Objects - Your Secret Performance Weapon.....	325
Geo Policy vs. GEO Updatable Objects.....	326
Wrap-up Discussion and Additional Resources.....	328

Welcome & Introduction

- Your Instructor: **Timothy Hall, CISSP, CCSM Elite, CCSI**
 - 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](#) (3,000+), [Link to all CPUG.org posts](#) (2,200+)
 - Creator of the self-guided video training series "Max Capture: Know Your Packets" & "Gaia 3.10 Immersion"
 - Author of Book “Max Power 2020: Check Point™ Firewall Performance Optimization”



The screenshot shows the Amazon product page for the book "Max Power 2020: Check Point Firewall Performance Optimization". The book cover features a blue and orange design with the title and author's name. The product title is "Max Power 2020: Check Point Firewall Performance Optimization: Foreword by Dameon D. Welch-Abernathy a.k.a. PhoneBoy". The author is Timothy C. Hall, and the foreword is by Dameon D. Welch-Abernathy. The book is a paperback, published on January 12, 2020, and is priced at \$59.95. The page includes a "Look inside" button, a star rating of 4.5 stars from 15 ratings, and a "See all formats and editions" link. The paperback format is highlighted with a price of \$59.95 and a Prime logo. There are two new copies available for \$59.95 each. The page also features a "Buy new" section with a price of \$59.95, a Prime logo, and a "FREE delivery" date of Saturday, Aug 14. The book is in stock, and there are "Add to Cart" and "Buy Now" buttons. The page includes a "Secure transaction" badge, shipping and sales information from Amazon.com, and a return policy. There are also social media sharing options at the bottom.

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... 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

Gateway Performance Optimization Class Details

- **Prerequisites:** Minimum CCSE certification and at least 3 years experience working with Check Point™ gateways in a production environment. Preferred: Minimum 5 years of experience working with Check Point™ gateways on a production environment and knowledge of SecureXL and CoreXL.
- We will be working with the R81.20 GA Check Point™ code. Differences in R81.20 vs. older code will be highlighted; about 90% of the total class material also applies to R81.10 and earlier versions roughly back to version R80.40. R80.30 and earlier code versions are no longer officially supported by Check Point™.
- Your lab exercises are in a break/fix format. A number of issues and badly-optimized configurations based on real-world problems were introduced to your lab environment prior to class and will be rectified as you proceed through the lab exercises, running speed tests along the way to gauge the effectiveness and performance gain of your optimizations.
- The main focus of this course is the R81.20 code running on Check Point™ appliances (models 2200-28XXX), open hardware, and Maestro/Scalable Platforms (whose differences are covered by an appendix). VSX is not included. Most class material will also apply to Quantum Spark appliances (SMB models 1200-1800); some limited reference links will be provided for Quantum Spark/SMB appliances. For a great optimization guide specifically crafted for the SMB/Spark appliances, see this truly excellent CheckMates article by Hristo Grigorov: [Brief introduction to SMB performance tuning](#).
- The material presented in this course will mostly apply to CloudGuard gateways subject to the specific limitations detailed in [sk174965: Check Point™ Quantum R81.20 \(Titan\) Release 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 1 – R81.20 Performance Introduction & Concepts
- Module 2 – Network Level Optimization
- Module 3 – Basic Gaia 3.10/RHEL Optimization
- Module 4 – ClusterXL Performance Tuning
- Module 5 – CoreXL & Multi-Queue
- Module 6 – SecureXL Throughput Acceleration
- Module 7 – Access Control Policy Tuning
- Module 8 – Threat Prevention Policy Tuning
- Module 9 – HTTPS Inspection Optimization
- Module 10 – Heavy Connections/Elephant Flows & HyperFlow/Pipeline Processing
- Appendix A – Intermittent/Historical Performance Issues Investigation & Monitoring
- Appendix B – Maestro/Scalable Platforms Commands
- Appendix C – GEO Updatable Objects - Your Secret Performance Weapon