Shadow Peak
SECURITY TRAINING AND SERVICES

Gateway Performance Optimization

Timothy C. Hall, Shadow Peak Inc.

CHECK POINT™

Check Point mind
Learn from the masters!

Table of Contents

Welcome & Introduction....9

Gateway Performance Optimization Class Details....10

List of Class Modules....11

Module 1 – R81.20 Performance Introduction & Concepts....12

Introduction....12

Background: Check Point™ History & Architecture....12

Your Best Friend: GA Jumbo Hotfix Accumulators....14

Useful Performance-Related CheckMates Community Tools....14

The “Super Seven” Performance Assessment Commands....15

“Super Seven” in the SmartConsole....16

Common Check Point™ Commands (ccc) by Danny Jung....17

CheckMates “One-Liners”....18

Gateway Performance Optimization Lab Tips....22

Beware: Speed Tests & Client-based AntiMalware/AntiVirus Software....25

Lab Exercise 1: Explore the Lab Environment, Initial Speed Tests, & CheckMates Community Tools....26

Explore the Current Configuration in the SmartConsole....26

Execute Initial Speed Tests and Note Awful Performance....28

Work with ccc and s7pac “Super Seven”....30

Module 2 – Network Level Optimization....33

Background....33

Latency/Jitter vs. Loss....33

Packets/sec vs. Throughput....35

New Connection Rates & Rulebase Lookups....38

Measuring Firewall Latency....39

IP Fragments Effect on Performance....40

The RX “Dark Triad”....42

Network Interface Stability, Error Counters, & Interface Speed Checks....42

Mitigating Overruns (RX-OVR): Interface Bonding....43

Special Case: RX-OVR and RX-DRP Increment in "Lockstep"....45

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

Other Network Interface Errors: RX-ERR....45
What about RX-DRP?....45
Network Driver Updates – Look Out!....46
ARP Neighbor Table Overflows....47
Asymmetric Path Issues & Traceroute....48
IP Routing Convergence Issues....49
Lab Exercise 2: Diagnose & Correct Network Performance Issues....51
Execute Failover and Run Speed Tests Again....51
Fail back Over and Troubleshoot High Latency....52
Measure Firewall Latency & Continue Troubleshooting....53
Troubleshoot Bandwidth Issues....54
Troubleshoot Packet Loss....55
Check Firewall Network Counters....55
Correct External Network Issues....56
Module 3 – Basic Gaia 3.10/RHEL Optimization....62
Background....62
Gaia 3.10 Kernel Updates....62
Introduction: User Space Firewall (USFW)....62
The “top” & “free” Gaia/Linux Commands....66
Top Output: “us” & “ni” – Process/User Space....67
Top Output: “sy” &”si” – System Space....68
Top Output: “wa” – Waiting for I/O Operation....68
Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles....69
CPU Usage Spikes: Introducing the Spike Detective....69
Firewall Hardware Health Check & Weird CPU Usage....71
Gaia Memory Management....72
Check Point™ Specific Commands....73
Memory Allocation Failures....74
Connection Table Overflows....75
A “Second Opinion” - The sar Command....79
HealthCheck Point™ (HCP)....82

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

Lab Exercise 3: Examine Gaia Health & Optimize....84
Run HealthCheck Point™....84
Run healthcheck.sh....86
Unlock & Run "Secret" hcp Performance Reports....86
Launch Policy Installation and Observe Waiting for I/O....88
Resolve Memory Shortages....91
Run Speed Tests and Observe Core Utilization....94
Launch Port Scan and Observe Connection Table Behavior....94
Module 4 – ClusterXL Performance Tuning....98
A Quick Note: SDF and the Correction Layer....98
Sync Network Health Check....98
Selective Synchronization of Services & Delayed Sync....100
Verifying Proper Cluster Operation....103
The "Cluster Under Load" Mechanism....103
Lab Exercise 4: Verify Cluster Operation & Sync Network Health....104
Checking Cluster Status....104
Cause a Catastrophic Failover and Observe Behavior....104
Cause a Non-Catastrophic Failover and Observe Behavior....107
Check & Correct Sync Network Health....107
Verify the Default Setting for Delayed Sync....110
Module 5 – CoreXL & Multi-Queue....111
Old School <R81: CoreXL "Static Split"....111
New School R81+: CoreXL Dynamic Balancing ("Dynamic Split")....113
RX-DRP & Ring Buffer Sizes....117
Multi-Queue Introduction....118
Multi-Queue Parallel Queues Limitations....119
The Dynamic Dispatcher & Priority Queueing....121
SND/IRQ Core Balancing....123
Lab Exercise 5: Multi-Queue, CoreXL Splits, and Static CoreXL Split Changes....126
Examine Multi-Queue Configuration....126
Correct Multi-Queue & Ring Buffer Issues....127

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

Work with the Dynamic Dispatcher/Priority Queues & Enable....128
Modifying the Static CoreXL Split....131
Module 6 – SecureXL Throughput Acceleration....135
SecureXL Introduction Part 1 - Throughput Acceleration....135
SecureXL Introduction Part 2 – Accept Templates....136
Throughput Acceleration – fwaccel stats -s....137
Accelerated conns/Total conns (Software Accept Template Match)....138
LightSpeed conns/Total Conns (Hardware Accept Template Match)....138
Accelerated pkts/Total pkts (Software Fastpath)....138
LightSpeed pkts/Total pkts (Hardware Fastpath)....138
F2Fed pkts/Total pkts....138
F2V pkts/Total pkts....139
CPASXL pkts/Total pkts....139
PSLXL pkts/Total pkts....139
CPAS Pipeline & PSL Pipeline....139
QOS inbound & outbound pkts/Total pkts....140
Corrected pkts/Total pkts....140
Core Type Responsibilities & Relative Process Path Efficiency....140
Path Optimization Strategy....141
Corner Case: High Acceleration Rates & SMT/Hyperthreading....142
Selectively Disabling SecureXL....143
Forcing SecureXL Acceleration with fast_accel....144
The "fwaccel conns", "fw_mux all", fw_streaming, & "fw ctl multik gconn" Commands....147
Processing Path Determination Techniques....147
The Easy Way: Trying to Use cpview to View Processing Path Determination Reason....148
The Hard Way: Performing a Kernel Debug....149
SecureXL Throughput Acceleration Limitations....150
New SecureXL Frontiers: LightSpeed & UPPAK....151
Lab Exercise 6: Observing SecureXL Behavior & Determining Why Traffic is F2F....153
Examine Throughput Acceleration Levels....153
Execute Debug to Determine Why Certain Traffic is F2F/slowpath....156

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

Remove Manual F2F Definition....158
Set Up Fast_Accel....161
Module 7 – Access Control Policy Tuning....163
Background....163
The Importance of a Properly Defined Firewall Topology....163
The Special Policy Object “Internet” & APCL/URLF Rules....166
GEO Updatable Objects: Your Secret Performance Weapon....169
Geo Policy vs. GEO Updatable Objects....170
rad Daemon Scalability Issues w/ Large User Populations....171
Access Control Column-based Matching: “Any” is the Enemy....173
Beware: Use of Domain Objects, and Wildcards in Custom Application/Site Objects....175
SecureXL Session Rate Acceleration (Accept Templates)....177
The Few Services & Rulebase Conditions That Can Still Disable Accept Templating in R80.10+....178
SecureXL Drop Templates and the Penalty Box....182
NAT Policy Optimization....184
IPSec Site-To-Site VPN Performance Tuning....185
VPNs: 3DES vs. AES & AES New Instructions (AES-NI)....185
IPSec VPN Recommended Algorithms....186
VPNs: IPSec: Low MTUs & PMTUD....187
Lab Exercise 7: Object Internet, Accept Templates, Optimizing APCL/URLF Policies....190
APCL/URLF Policy Optimization....190
Optimize SecureXL Accept Templates....194
Configure & Test the SecureXL Penalty Box....197
NAT Optimization Exercise....201
VPN Optimization Exercise....204
Module 8 – Threat Prevention Policy Tuning....208
Introduction....208
Quickly Assessing IPS/Threat Prevention Performance Impact....208
IPS Inspection Coverage: TP Main Layer vs. Legacy “IPS” Layer....210
Cut to the Chase: hcp’s Secret TP Reports....211

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

Don’t Even Think About It: IPS Bypass Under Load....214
Performance Impact: Inactive vs. Prevent vs. Detect....214
Custom IPS Profile Optimization: IPS ThreatCloud & Core Activations....215
Custom Profile Optimization: Inspection Settings....217
Threat Prevention: “Null” Profiles vs. Blade-based Exceptions....217
Threat Prevention Blade-Based Exceptions....219
Threat Prevention "Null Profiles"....222
Custom vs. Autonomous TP Policy Management....224
Lab Exercise 8: Finding F2F TP traffic, Exceptions & Null Profiles....225
Diagnosing Threat Prevention Performance Issues....225
Disable Threat Prevention and Retest Performance....226
Run "Secret" hcp Threat Prevention Performance Reports....227
Examine SmartConsole Threat Prevention Configuration....230
Engage TP Profile Cleanup Options....231
Retest Performance after Optimizations....233
Create Blade-based Exception & Retest Speed....236
Module 9 – HTTPS Inspection Optimization....241
The Impact: Enabling HTTPS Inspection....241
Quick Mention: Outbound "Lite" Inspection a.k.a. Categorize HTTPS Sites....241
HTTPS Inspection Policy Optimization Best Practices....243
Lab Exercise 9: Optimize an HTTPS Inspection Policy....247
Identify Active Streaming Connections....247
Optimize Existing HTTPS Inspection Policy to Best Practices....249
Retest Active Streaming Performance After Optimizations....256
Verify HTTPS Inspection Policy Operation....258
Module 10 – Heavy Connections/Elephant Flows & HyperFlow/Pipeline Processing....260
Identifying Elephant/Heavy Connections....260
Remediating Elephant Flows....261
SecureXL Rate Limiting & Network Quotas....262
SecureXL and the Quality of Service (QoS) Blade....263

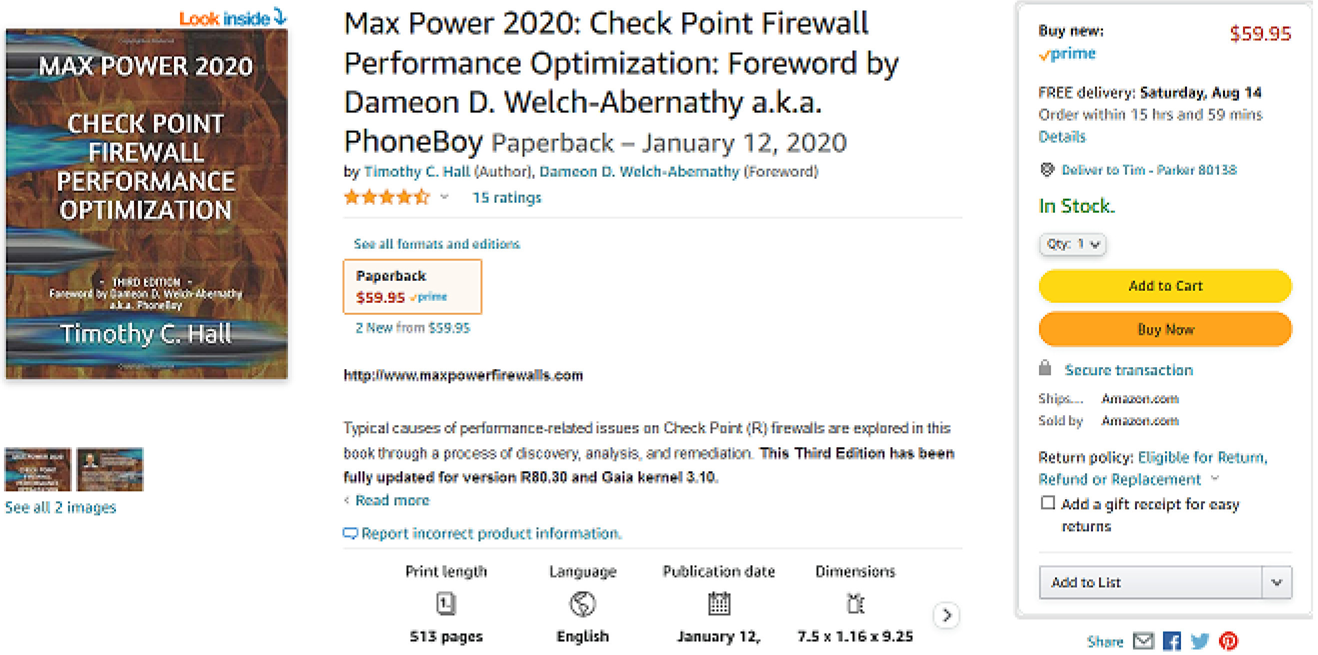
Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

R81.20: HyperFlow & the "Pipeline" SecureXL Paths....263
HyperFlow Example....267
Monitoring/Configuring HyperFlow – CLI Commands....270
Monitoring HyperFlow – cpview....271
Monitoring HyperFlow – SmartConsole....274
Lab Exercise 10: Heavy Connections, Dynamic Split & HyperFlow....275
Create Multiple Elephant Flows & View Statistics....275
Enable Dynamic Balancing/Split & Hyperflow....277
Test Dynamic Split....278
Test HyperFlow/Pipeline Processing....282
Enforce Rate Limits....288
Appendix A – Intermittent/Historical Performance Issues Investigation & Monitoring....291
Syslog – A Frequently Effective Shortcut....291
cpview History Mode....292
New Monitoring Frontiers – Skyline....293
Getting a "Second Opinion": The sar Command....295
Check the Spike Detective....296
What Else Changed?....296
SmartView Monitor Reports....296
Optional Lab: cpview History Mode & the sar Command....297
cpview Historical Mode....298
Getting a “Second Opinion” from the CLI with sar....298
Appendix B – Maestro/Scalable Platforms Commands....300
Live Performance Overview: asg perf -vp....300
Finding Performance "Hogs": asg_perf_hogs....302
Diagnostics for Scalable Platforms/Maestro: asg diag....303
Setting Limits with Session Control Rules: asg_session_control....304
Finding Which SGM (and path) is Handling a Degraded Connection: asg search....305
Packet Distribution Issues Between SGM’s: show distribution....306
Wrap–up Discussion and Additional Resources....307

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

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 (3,000+), Link to all CPUG.org posts (2,200+)
  - Creator of the self-guided video training series "Check Point™ IPS/AV/ABOT Immersion", "Gaia 3.10 Immersion" and "Max Capture: Know Your Packets"
  - Author of Book “Max Power 2020: Check Point™ Firewall Performance Optimization”


Look inside
MAX POWER 2020
CHECK POINT FIREWALL PERFORMANCE OPTIMIZATION
THIRD EDITION
Foreword by Dameon D. Welch-Abernathy a.k.a. PhoneBoy
Timothy C. Hall
See all 2 images

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

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

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). Most class material will also apply to Quantum Spark appliances (models 1200-1800); some limited reference links will be provided for Quantum Spark appliances. VSX is not included.
- 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.

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7

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

Copyright 2023 Shadow Peak Inc. All rights reserved. Version 1.7