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....................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 Environment, 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
Packets/sec vs. Throughput....................37
New Connection Rates & Rulebase Lookups....................40
Measuring Firewall Latency....................41
IP Fragments Effect on Performance....................42
The RX “Dark Triad”....................44
Network Interface Stability, Error Counters, & Interface Speed Checks....................45
Mitigating Overruns (RX-OVR): Interface Bonding....................46
A Common Issue: Bond Traffic Imbalances!....................46

A Controversial Option: Ethernet Flow Control/Pause Frames 47
Special Case: RX-OVR and RX-DRP Increment in "Lockstep" 47
Other Network Interface Errors: RX-ERR 48
Clearing Network Counters 48
What about RX-DRP? 48
Network Driver Updates – Look Out! 48
ARP Neighbor Table Overflows 50
Asymmetric Path Issues & Traceroute 51
IP Routing Convergence Issues 52
Lab Exercise 2: Diagnose & Correct Network Performance Issues 54
Execute Failover and Run Speed Tests Again 54
Fail back Over and Troubleshoot High Latency 55
Measure Firewall Latency & Continue Troubleshooting 56
Troubleshoot Bandwidth Issues 57
Troubleshoot Packet Loss 58
Check Firewall Network Counters 58
Correct External Network Issues 59
Module 3 – Basic Gaia 3.10/RHEL Optimization 65
Background 65
Gaia 3.10 Kernel Updates 65
Introduction: User Space Firewall (USFW) 65
The “top” & “free” Gaia/Linux Commands 69
Top Output: “us” & “ni” – Process/User Space 70
Top Output: “sy” &”si” – System Space 71
Top Output: “wa” – Waiting for I/O Operation 71
Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles 72
CPU Usage Spikes: Introducing the Spike Detective 73
Firewall Hardware Health Check & Weird CPU Usage 74
Gaia Memory Management 76
Check Point™ Specific Commands 77
Memory Allocation Failures 77

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

Connection Table Overflows....79
Special Case: Maestro & Connection Table Overflows....83
A “Second Opinion” - The sar Command....84
HealthCheck Point™ (HCP)....87
Lab Exercise 3: Examine Gaia Health & Optimize....89
Run HealthCheck Point™....89
Run healthcheck.sh....91
Unlock & Run "Secret" hcp Performance Reports....91
Launch Policy Installation and Observe Waiting for I/O....93
Resolve Memory Shortages....96
Run Speed Tests and Observe Core Utilization....99
Launch Port Scan and Observe Connection Table Behavior....99
Module 4 – ClusterXL Performance Tuning....103
A Quick Note: SDF and the Correction Layer....103
Sync Network Health Check....103
Selective Synchronization of Services & Delayed Sync....105
Verifying Proper Cluster Operation....108
The "Cluster Under Load" Mechanism....108
Lab Exercise 4: Verify Cluster Operation & Sync Network Health....109
Checking Cluster Status....109
Cause a Catastrophic Failover and Observe Behavior....109
Cause a Non-Catastrophic Failover and Observe Behavior....112
Check & Correct Sync Network Health....112
Verify the Default Setting for Delayed Sync....115
Module 5 – CoreXL & Multi-Queue....116
Old School <R81: CoreXL "Static Split"....116
New School R81+: CoreXL Dynamic Balancing ("Dynamic Split")....118
RX-DRP & Ring Buffer Sizes....122
Multi-Queue Introduction....124
Multi-Queue Parallel Queues Limitations....124
The Dynamic Dispatcher & Priority Queueing....126
SND/IRQ Core Balancing....129

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

Tracking Down Unexplained High CPU Usage: The Undocumented "perf" Command....131
Scenario 1: Persistent, Excessive CPU Utilization by a Process....132
Scenario 2: Persistent, Excessive CPU Utilization on a Particular Core....134
CoreXL Frontiers: Intel’s "P-Cores" & "E-Cores"....136
Lab Exercise 5: Multi-Queue, CoreXL Splits, and Static CoreXL Split Changes....137
Examine Multi-Queue Configuration....137
Correct Multi-Queue & Ring Buffer Issues....138
Work with the Dynamic Dispatcher/Priority Queues & Enable....139
Modifying the Static CoreXL Split....142
Module 6 – SecureXL Throughput Acceleration....146
SecureXL Introduction Part 1 - Throughput Acceleration....146
SecureXL Introduction Part 2 – Accept Templates....147
Throughput Acceleration – fwaccel stats -s....148
Accelerated conns/Total conns (Software Accept Template Match)....149
LightSpeed conns/Total Conns (Hardware Accept Template Match)....149
Accelerated pkts/Total pkts (Software Fastpath)....149
LightSpeed pkts/Total pkts (Hardware Fastpath)....149
F2Fed pkts/Total pkts....149
F2V pkts/Total pkts....150
CPASXL pkts/Total pkts....150
PSLXL pkts/Total pkts....150
CPAS Pipeline & PSL Pipeline....150
QOS inbound & outbound pkts/Total pkts....151
Corrected pkts/Total pkts....151
Core Type Responsibilities & Relative Process Path Efficiency....151
Path Optimization Strategy....154
Corner Case: High Acceleration Rates & SMT/Hyperthreading....154
Selectively Disabling SecureXL....156
Forcing SecureXL Acceleration with fast_accel....157
The "fwaccel conns", "fw_mux all", fw_streaming, & "fw ctl multik gconn" Commands....159
Processing Path Determination Techniques....160
The Easy Way: "fw tab -t connections -z" and cpview....160
The Hard Way: Performing a Kernel Debug....162

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

SecureXL Throughput Acceleration Limitations....163
SecureXL Frontiers: LightSpeed & UPPAK....164
Lab Exercise 6: Observing SecureXL Behavior & Determining Why Traffic is F2F....166
Examine Throughput Acceleration Levels....166
Execute Debug to Determine Why Certain Traffic is F2F/slowpath....169
Remove Manual F2F Definition....171
Set Up Fast_Accel....174
Module 7 – Access Control Policy Tuning....176
Background....176
The Importance of a Properly Defined Firewall Topology....176
The Special Policy Object “Internet” & APCL/URLF Rules....179
GEO Updatable Objects: Your Secret Performance Weapon....182
Geo Policy vs. GEO Updatable Objects....183
rad Daemon Scalability Issues w/ Large User Populations....184
Access Control Column-based Matching: “Any” is the Enemy....186
Beware: Use of Domain Objects, and Wildcards in Custom Application/Site Objects....188
SecureXL Session Rate Acceleration (Accept Templates)....190
The Few Services & Rulebase Conditions That Can Still Disable Accept Templating in R80.10+....191
SecureXL Drop Templates and the Penalty Box....195
NAT Policy Optimization....197
IPSec Site-To-Site VPN Performance Tuning....198
VPNs: 3DES vs. AES & AES New Instructions (AES-NI)....198
IPSec VPN Recommended Algorithms....199
VPNs: IPSec: Low MTUs & PMTUD....200
Lab Exercise 7: Object Internet, Accept Templates, Optimizing APCL/URLF Policies....203
APCL/URLF Policy Optimization....203
Optimize SecureXL Accept Templates....207
Configure & Test the SecureXL Penalty Box....210
NAT Optimization Exercise....214
VPN Optimization Exercise....217
Module 8 – Threat Prevention Policy Tuning....221

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

Introduction....221
Quickly Assessing IPS/Threat Prevention Performance Impact....221
IPS Inspection Coverage: TP Main Layer vs. Legacy “IPS” Layer....223
Cut to the Chase: hcp’s Secret TP Reports....224
IPS Bypass Under Load: Formerly Unusable But Now an Option....227
Performance Impact: Inactive vs. Prevent vs. Detect....227
Custom IPS Profile Optimization: IPS ThreatCloud & Core Activations....228
Custom Profile Optimization: Inspection Settings....230
Performance: IPS Blade vs. All Other Threat Prevention Blades....231
Threat Prevention: “Null” Profiles vs. Blade-based Exceptions....235
Threat Prevention Blade-Based Exceptions....236
Threat Prevention "Null Profiles"....239
Custom vs. Autonomous TP Policy Management....241
Lab Exercise 8: Finding F2F TP traffic, Exceptions & Null Profiles....242
Diagnosing Threat Prevention Performance Issues....242
Disable Threat Prevention and Retest Performance....243
Run "Secret" hcp Threat Prevention Performance Reports....244
Examine SmartConsole Threat Prevention Configuration....247
Engage TP Profile Cleanup Options....248
Retest Performance after Optimizations....251
Create Blade-based Exception & Retest Speed....254
Module 9 – HTTPS Inspection Optimization....259
The Impact: Enabling HTTPS Inspection....259
Quick Mention: Outbound "Lite" Inspection a.k.a. Categorize HTTPS Sites....259
HTTPS Inspection Policy Optimization Best Practices....261
Lab Exercise 9: Optimize an HTTPS Inspection Policy (Optional)....265
Identify Active Streaming Connections....265
Optimize Existing HTTPS Inspection Policy to Best Practices....267
Retest Active Streaming Performance After Optimizations....274
Verify HTTPS Inspection Policy Operation....277

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15
For Attendee’s Personal Use Only – Do Not Distribute

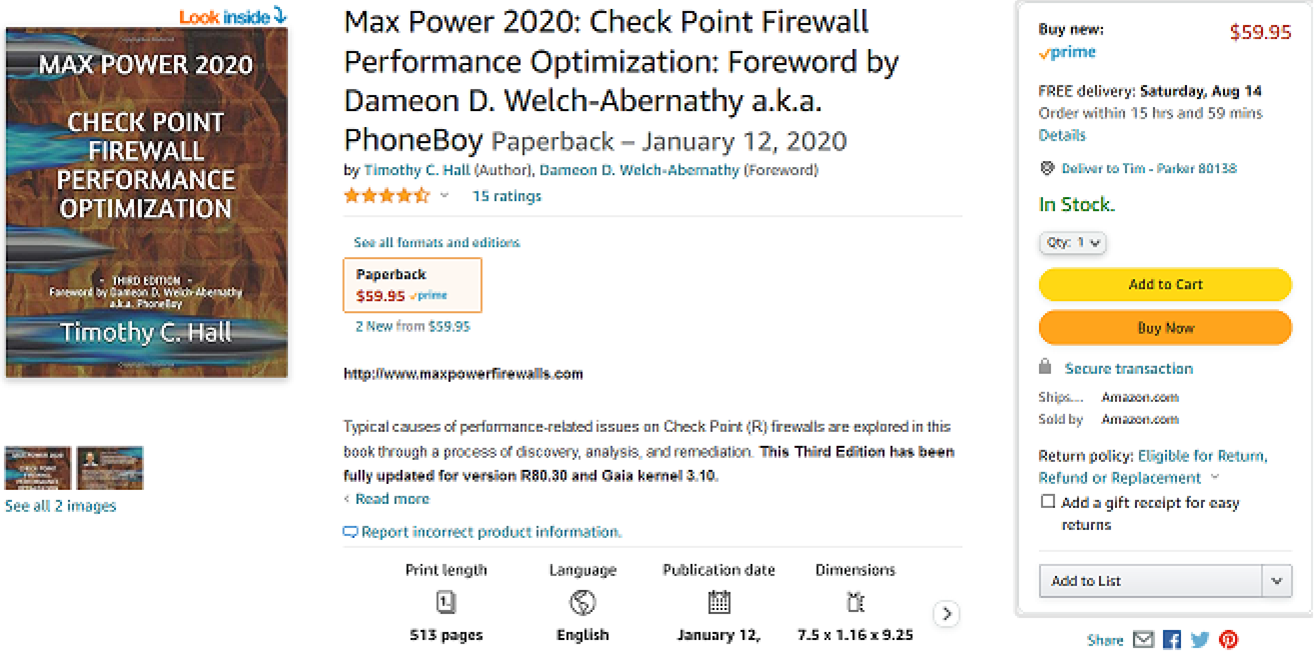
Module 10 – Heavy Connections/Elephant Flows & HyperFlow/Pipeline Processing....279
Identifying Elephant/Heavy Connections....279
Remediating Elephant Flows....280
SecureXL Rate Limiting & Network Quotas....281
SecureXL and the Quality of Service (QoS) Blade....282
R81.20: HyperFlow & the "Pipeline" SecureXL Paths....282
HyperFlow Example....286
Monitoring/Configuring HyperFlow – CLI Commands....290
Monitoring HyperFlow – cpview....291
Monitoring HyperFlow – SmartConsole....294
Lab Exercise 10: Heavy Connections, Dynamic Split & HyperFlow....295
Create Multiple Elephant Flows & View Statistics....295
Enable Dynamic Balancing/Split & Hyperflow....297
Test Dynamic Split....298
Test HyperFlow/Pipeline Processing....302
Enforce Rate Limits....308
Appendix A – Intermittent/Historical Performance Issues Investigation & Monitoring....311
Syslog – A Frequently Effective Shortcut....311
cpview History Mode....312
New Monitoring Frontiers – Skyline....313
Getting a "Second Opinion": The sar Command....315
Check the Spike Detective....316
What Else Changed?....316
SmartView Monitor Reports....317
Optional Lab: cpview History Mode & the sar Command....318
cpview Historical Mode....319
Getting a “Second Opinion” from the CLI with sar....319
Appendix B – Maestro/Scalable Platforms Commands....321
Live Performance Overview: asg perf -vp....321
Finding Performance "Hogs": asg_perf_hogs....323

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

Diagnostics for Scalable Platforms/Maestro: asg diag....324
Setting Limits with Session Control Rules: asg_session_control....325
Finding Which SGM (and path) is Handling a Degraded Connection: asg search....326
Packet Distribution Issues Between SGM's: show distribution....327
Wrap–up Discussion and Additional Resources....328

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 "Max Capture: Know Your Packets" & "Gaia 3.10 Immersion"
  - Author of Book “Max Power 2020: Check Point™ Firewall Performance Optimization”



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

Secure transaction

Ships...	Amazon.com
Sold by	Amazon.com

Return policy: Eligible for Return, Refund or Replacement

□ Add a gift receipt for easy returns

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

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.

Copyright 2024 Shadow Peak Inc. All rights reserved. Version 1.15

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 2024 Shadow Peak Inc. All rights reserved. Version 1.15