

Table of Contents

List of Figures.....	xiii
List of Tables.....	xx
Foreword.....	xxi
Preface.....	xxiii
Why Was This Book Created?.....	xxiii
Fourth Edition Notes.....	xxiv
How to Use This Book.....	xxv
Conventions.....	xxvii
And Now for a Word.....	xxviii
About the Author.....	xxix
Chapter 1 R82.10 Introduction & Concepts.....	31
Introduction.....	31
Background: Check Point™ History & Architecture.....	32
The "Thin Pink Line" of Check Point™ & Effective Troubleshooting.....	32
Methodology.....	34
Your Best Friend: GA Jumbo Hotfix Accumulators.....	34
Official Tools: cpview and hcp.....	36
HealthCheck Point™ (hcp).....	37
Easily Accessing hcp Results in a Web Browser.....	39
The "Secret" TAC Tests.....	41
CheckMates Community Tools & "One-Liners".....	42
The "Super Seven" Performance Assessment Commands.....	42
The "Super Seven" in the SmartConsole GUI.....	43
Common Check Point™ Commands (ccc).....	44
Dynamic Changes Pushed to Firewalls by Check Point™ & Data Sharing.....	47
Threat Prevention and Application Control Updates.....	48

The AutoUpdater, CPDiag Service, & Check Point™ Live Patch.....	50
Maestro Dynamic Release Updates.....	51
Data Sharing Settings.....	51
Tip: Network Topology Discovery with hcp, CDP, and LLDP.....	52
Determining the Busiest Times of Day.....	55
Speed Testing Tips.....	58
For Labs Only: Turning the Gaia OS Into a Pure Router.....	59
R82.10 Introduction & Concepts: Key Points.....	60
Chapter 2 OSI Layers 1&2 Performance Optimization.....	61
Background.....	61
Discovery.....	62
NIC Hardware & Drivers: Intel & Mellanox/NVIDIA.....	64
Stick with Intel or Mellanox/NVIDIA NICs.....	66
Network Interface Stability, Error Counters, & Interface Speed Checks.....	67
Watch Out: Non-standard Firewall Interface MTUs.....	69
A Millisecond in the Life of a Frame.....	70
IP Fragments Effect on Performance.....	73
The RX “Dark Triad”.....	74
Mitigating Overruns (RX-OVR): Interface Bonding.....	76
A Common Issue: Bond Traffic Imbalances!.....	76
A Controversial Option: Ethernet Flow Control/Pause Frames.....	77
Special Case: RX-OVR and RX-DRP Increment in "Lockstep".....	78
Other Network Interface Errors: RX-ERR.....	78
Clearing Network Counters.....	79
What about RX-DRP?.....	79
Increasingly Rare, but Still Deadly at 100Mbps: Duplex Mismatches.....	80
Firewall Hardware Health Check.....	81
Firewall Open Hardware BIOS Tuning & NUMA.....	84
NUMA Considerations for Check Point™ Firewall Appliances.....	86
NUMA Considerations for Open Hardware/Server Firewalls.....	87
Spanning Tree Protocol (STP) Sanity Check.....	88
IPv4 ARP Neighbor Table Overflows.....	93

IPv6 and the Neighbor Discovery Protocol.....	98
OSI Layers 1&2 Performance Optimization: Key Points.....	99
Chapter 3 OSI Layer 3 Performance Optimization.....	101
Background.....	101
Static vs. Dynamic Routing.....	101
Mismatched Subnet Masks in the Same IP Subnet.....	102
Core Router Supernet Loops.....	104
ICMP: Canary in the Coal Mine.....	107
Latency/Jitter vs. Loss.....	108
Latency/Jitter/Loss – The Speed Test Impact.....	109
Network Measurement/Probing Tools – ping/tracert/traceroute/pathping/mtr.....	109
Crafting Traffic to Test Policy/NAT and Routing Connectivity.....	114
Testing Policy Changes and Packet Tracing.....	118
New Connection Rates & Rulebase Lookups.....	119
Measuring Firewall Latency & Application Performance.....	120
Application Connection Timeouts.....	122
OSI Layer 3 Performance Optimization: Key Points.....	125
Chapter 4 Gaia OS 3.10/4.18/5.14 Optimization.....	127
Background.....	127
Gaia Kernel Updates.....	127
The Importance of Properly Defined DNS Servers in Gaia.....	128
User Space Firewall (USFW) and its Impact on CPU Utilization.....	130
Introduction: User Space Performance Pack (UPPAK).....	134
The “top” & “free” Gaia/Linux Commands.....	135
Before We Begin: Ignore the "Load Average" Numbers.....	137
Top Output: “us” & “ni” – Process/User Space.....	138
Top Output: “sy” & “si” – System Space.....	139
Top Output: “wa” – Waiting for I/O Operation (The "Bad Guy").....	139
Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles.....	141
CPU Usage Spikes: Introducing the Spike Detective.....	142
Gaia Memory Management.....	143
Firewall Disk Space Check.....	146

Solid State Drive (SSD) Considerations.....	146
Check Point™ Specific Commands.....	147
Memory Allocation Failures.....	147
Connection Table Overflows.....	149
Special Case: Maestro/ElasticXL & Connection Table Overflows.....	156
Gaia OS 3.10/4.18/5.14 Optimization: Key Points.....	158
Chapter 5 ClusterXL/Maestro/ElasticXL Performance Tuning.....	159
Background.....	159
Make the Call: Where to Focus in this Chapter (or not).....	160
Sticky Decision Function (SDF) and the New Correction Layer.....	161
Maestro vs. ElasticXL.....	161
Maestro/ElasticXL Distribution & Correction.....	162
Sync Network Health Check.....	164
Selective Synchronization of Services & Delayed Sync.....	166
Verifying Proper ClusterXL Operation.....	171
The "Cluster Under Load" Mechanism.....	172
Troubleshooting “Slow” Failovers.....	172
STP and Portfast.....	173
Dynamic Routing & “Wait for Clustering”.....	173
Cluster Member Recovery Mode Setting.....	174
Connections Survive Failovers, Mostly.....	176
Miscellaneous ClusterXL/Maestro/ElasticXL Performance Topics.....	178
ClusterXL/Maestro/ElasticXL Performance Tuning: Key Points.....	180
Chapter 6 CoreXL & Multi-Queue.....	181
Background.....	181
Discovery.....	182
Scenario 1: CoreXL enabled with Dynamic Split, SecureXL enabled.....	184
Scenario 2: CoreXL enabled with Static Split, SecureXL enabled.....	184
Scenario 3: CoreXL off, SecureXL enabled.....	184
Scenario 4: CoreXL enabled with Static/Dynamic Split, SecureXL disabled.....	185
Old School <R81: CoreXL "Static Split".....	185
New School R81+: CoreXL Dynamic Balancing ("Dynamic Split").....	189

Dynamic Split Support Requirements & Troubleshooting.....	190
Monitoring Dynamic Split.....	191
VSX: Static vs. Dynamic Split Philosophy.....	194
The "Green" Power-Saving Feature (R82.10).....	196
RX-DRP & Ring Buffer Sizes.....	196
Impact of Oversized Ring Buffers with KPPAK – An Example.....	200
Multi-Queue Introduction.....	202
Multi-Queue Parallel Queues Limitations.....	203
The Dynamic Dispatcher & Priority Queueing.....	207
SND Core Balancing.....	211
Tracking Down Unexplained High CPU Usage: The "perf" Command.....	215
Troubleshooting Persistent, Excessive CPU Utilization on a Particular Core.....	216
CoreXL Frontiers: Intel's P-Cores & E-Cores.....	220
CoreXL & Multi-Queue: Key Points.....	222
Chapter 7 SecureXL Throughput Acceleration.....	223
Background.....	223
Check for Manual Interface Affinity.....	223
Introduction to UPPAK.....	225
SecureXL Introduction Part 1 – Throughput Acceleration.....	225
SecureXL Introduction Part 2 – Accept Templates.....	227
Throughput Acceleration – fwaccel stats -s.....	228
Accelerated conns/Total conns (Software Accept Template Match).....	230
LightSpeed conns/Total conns (Hardware Accept Template Match).....	230
Accelerated pkts/Total pkts (Software Fastpath).....	230
LightSpeed pkts/Total pkts (Hardware Fastpath).....	230
F2Fed pkts/Total pkts (Slowpath).....	231
F2V pkts/Total pkts.....	231
CPASXL pkts/Total pkts (Medium Path, Active Streaming).....	232
PSLXL pkts/Total pkts (Medium Path, Passive Streaming).....	232
UDP IS XL & UDP IS pipeline pkts/Total pkts (R82+ only).....	233
CPAS Pipeline & PSL Pipeline (HyperFlow).....	233
QOS inbound & outbound pkts/Total pkts.....	233

Corrected pkts/Total pkts (Maestro/ElasticXL Only).....	233
Core Type Responsibilities & Relative Process Path Efficiency.....	234
Path Optimization Strategy.....	237
Corner Case: High Acceleration Rates & SMT/Hyperthreading.....	238
Selectively Disabling SecureXL.....	238
Forcing SecureXL Acceleration with fast_accel.....	240
Example fast_accel Configuration.....	242
R81.20 and Earlier – Processing Path Location Commands.....	245
R82+ Path Location with connview.....	248
Determining Reason for Slowpath (F2F) Traffic.....	249
The Easy Way: fw tab -t connections -z.....	249
The Hard Way: Performing a Kernel Debug.....	250
SecureXL Throughput Non-Acceleration (Slowpath) Reasons.....	252
SecureXL Throughput Acceleration: Key Points.....	256
Chapter 8 Brave New World: UPPAK.....	257
Introduction.....	257
UPPAK & USFW – Two Very Different but Similar-sounding Features.....	257
First SecureXL Revamp: R70 and CoreXL.....	258
Second SecureXL Revamp: R80.20.....	259
Third SecureXL Revamp: User Space Performance Pack (UPPAK).....	260
UPPAK Motivations & Improvements.....	261
Motivation #1: Firewall Stability.....	261
Motivation #2: Stop Drowning in an Onslaught of Interrupts.....	262
Motivation #3: Improve Software Processing Performance.....	263
Motivation #4: Introduce Hardware Offload Possibilities.....	265
Discovery.....	266
Force/LightSpeed Appliances & UPPAK.....	268
UPPAK Default State.....	268
UPPAK Feature Limitations & Behavioral Changes.....	269
UPPAK Troubleshooting.....	271
For Labs Only: UPPAK Poll Sleep Mode.....	272
Alternatives to Poll Sleep Mode.....	274

UPPAK Frontiers – Hardware Offloads.....	275
Brave New World: UPPAK Key Points.....	277
Chapter 9 Access Control Policy Tuning.....	279
Background.....	279
The Importance of a Properly Defined Firewall Topology.....	279
Making Topology Corrections.....	282
The Special Policy Object “Internet” & APCL/URLF Rules.....	284
Access Control Logging Options and Their Impact on Performance.....	288
Content Awareness Performance Tips.....	293
RAD Daemon Scalability Issues with Large User Populations.....	294
URL Filtering and the RAD Daemon.....	295
Access Control Rules: Column-based Matching.....	296
Use of Domain Objects and Wildcards in Custom Application/Site Objects.....	297
SecureXL Session Rate Acceleration (Accept Templates).....	301
Rulebase Conditions That Can Still Disable Accept Templating in R80.10+.....	303
But Wait, The Actual Accept Templating Rate is Always Zero?.....	305
Cause #1: Enabling Blades other than "Firewall" in the Top/Parent Layer.....	305
Cause #2: Use of "Protocol Signature" Option on Service Objects.....	308
Zero Accept Template Rate Diagnosis: fwaccel templates -R.....	310
SecureXL Optimized Drops.....	311
The SecureXL Penalty Box.....	314
NAT Policy Optimization.....	317
All You Can Eat: Geographic Enforcement & External Feeds.....	321
Legacy Geo Policy.....	322
Geo Updatable Objects.....	324
External Network Feeds.....	325
Access Control Policy Tuning: Key Points.....	328
Chapter 10 IPsec VPN Optimization.....	329
Make the Call: Where to Focus in this Chapter (or not).....	329
IPsec VPN Background & Performance Tuning.....	330
VPNs: 3DES vs. AES & AES New Instructions (AES-NI) & GCM.....	330
IPsec Site-To-Site VPNs: Low MTUs & PMTUD.....	333

Balancing IPsec Traffic on SNDs: igb/ixgbe/ice Driver Issues.....	337
Permanent Tunnels & Dead Peer Detection (DPD).....	337
Diffie-Hellman, PFS, PQC, & VPN Tunnel Sharing.....	339
Post-Quantum Cryptography (PQC) in R82+.....	343
PQC Performance Considerations.....	343
Disabling SecureXL Acceleration of IPsec VPN Tunnels.....	344
IPsec Remote Access VPN Performance.....	346
The Impact of Visitor Mode.....	350
Check Point™ SASE Performance Considerations.....	352
IPsec VPN Optimization: Key Points.....	355
Chapter 11 Threat Prevention Policy Tuning.....	357
Introduction.....	357
Make the Call: Where to Focus in this Chapter (or not).....	358
Quickly Assessing IPS/Threat Prevention Performance Impact.....	358
IPS Inspection: TP Main Custom Layer vs. Legacy “IPS” Layer.....	361
Cut to the Chase: hcp’s "Secret" TP Report.....	363
IPS Bypass Under Load (R82 and Earlier).....	364
Adaptive IPS (R82.10).....	365
Performance Impact Ratings.....	369
Performance Impact of Actions: Inactive vs. Prevent vs. Detect.....	370
Custom IPS Profile Optimization: IPS ThreatCloud & Core Activations.....	370
Custom Profile Optimization: Inspection Settings.....	373
Performance: IPS Blade vs. Anti-Virus.....	373
Anti-Virus: Deep Scanning and Archive Scanning Considerations.....	375
What about Anti-Bot, Threat Emulation/Extraction, & Zero Phishing?.....	378
Threat Prevention: Global Blade-based Exceptions vs. Null Profiles.....	379
Threat Prevention Global Blade-based Exceptions.....	381
Threat Prevention Null Profiles.....	383
Custom vs. Autonomous TP Policy Management.....	385
Threat Prevention Policy Insights (R82.10).....	386
Threat Prevention Performance Frontiers – SmartNIC Hardware Offloads.....	388
Threat Prevention Policy Tuning: Key Points.....	389

Chapter 12 HTTPS Inspection & Active Streaming.....	391
Make the Call: Where to Focus in this Chapter (or not).....	391
HTTPS Inspection Overview.....	391
The Impact: Enabling HTTPS Inspection.....	392
Quick Mention: Categorize HTTPS Sites a.k.a. HTTPS "Lite Inspection".....	393
HTTPS Outbound Inspection Policy Optimization Best Practices.....	395
HTTPS Inspection Policy Overall Tips & Tricks.....	397
HTTPS Inspection Policy Performance-related Tips & Tricks.....	400
Frontiers for HTTPS Inspection in R82+.....	402
HTTPS Inspection & Active Streaming: Key Points.....	406
Chapter 13 Heavy (Elephant) Connections & HyperFlow.....	407
Background & Symptoms.....	407
Identifying Elephant/Heavy Connections.....	408
Remediating Elephant Flows.....	412
SecureXL Rate Limiting & Network Quotas.....	413
SecureXL and the Quality of Service (QoS) Blade.....	415
HyperFlow in R81.20+.....	415
The Three "Pipeline" Paths.....	416
HyperFlow Prerequisites and Requirements.....	417
HyperFlow Boosting Capabilities & Limitations.....	418
For Labs Only: Enabling HyperFlow on Open Hardware/VMWare.....	420
HyperFlow Example.....	420
Monitoring/Configuring HyperFlow – CLI Commands.....	424
Monitoring HyperFlow – cpview’s Advanced...HyperFlow Screen.....	427
Monitoring HyperFlow – SmartConsole.....	429
Management Data Plane Separation.....	430
Heavy (Elephant) Connections & HyperFlow: Key Points.....	433
Chapter 14 Intermittent Performance Issues & Setting Proactive Alerts.....	435
Introduction.....	435
What’s The Story & hcp Tests.....	436
Syslog – A Frequently Effective Shortcut.....	438
History Mode for cpview.....	439

Getting a “Second Opinion” – The sar Command.....	441
Skyline.....	445
Check the Spike Detective.....	446
What Else Changed?.....	447
SmartView Historical Report Graphs.....	448
Check the Firewall Traffic Logs.....	451
Setting Firewall Thresholds & Proactive Alerts.....	453
First Things First: Types of Alerts and Where to Send Them.....	453
Aggressive Aging Activation Alert.....	456
VPN Failure Notifications.....	458
Cluster Failover Alerts.....	460
Firewall Low Disk Space Alerts.....	461
Gaia-based SNMP Traps.....	461
DiagnosticsView – Offline Troubleshooting Using Only a cpinfo File.....	462
Intermittent Performance Issues & Setting Proactive Alerts: Key Points.....	464
Chapter 15 Final Thoughts – The Age of "AI".....	465
Appendix A – ElasticXL/Maestro/Scalable Platforms Commands.....	467
The New Command "insights" (R82+).....	468
Live Performance Overview: asg perf -vp.....	471
Finding Performance "Hogs": asg_perf_hogs.....	473
Diagnostics for Scalable Platforms/Maestro: asg diag.....	474
Setting Limits with Session Control Rules: asg_session_control.....	475
Finding Which Member is Handling a Degraded Connection: asg search.....	476
Maestro Packet Distribution Issues Between SGMs: show distribution.....	477
Appendix B – Additional Resources & Indexed CLI Quick Reference.....	479
Network/System Commands in Alphabetical Order – Gaia OS & Firewall.....	480