Table of Contents

List of Figures....................xiii

List of Tables....................xix

Foreword....................xxi

Preface....................xxiii
- Why Was This Book Created?....................xxiii
- Third Edition Notes....................xxiv
- How to Use This Book....................xxv
- Conventions....................xxvi
- And Now for a Word....................xxvii
- About the Author....................xxviii

Acknowledgments....................xxix

Chapter 1 R80.30 Introduction & Concepts....................31
- Introduction....................31
- Background: Check Point History & Architecture....................32
- Gaia 3.10 Kernel Update....................33
- Tip: Making Gaia Kernel Variable Adjustments....................33
- Your Best Friend: GA Jumbo Hotfix Accumulators....................34
- Methodology....................36
- Latency vs. Loss....................36
- Useful Performance-Related CheckMates Community Tools....................37
  - The “Super Seven” Performance Assessment Commands....................37
  - Common Check Point Commands (ccc)....................38
- Useful Performance-Related Tools Provided by Check Point....................38
  - healthcheck.sh....................38
  - cpsizeme....................41
  - cpview....................41
  - fw monitor & cppcap....................41

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Check Point Performance Test Results: 5600 Model....42
Performance Testing Environment Setup....43
Discovery....44
Network Device Health Check....48
Monitoring Blade Present?....49
Determining the Busiest Times of Day....52
R80.30 Introduction & Concepts: Key Points....55

Chapter 2 Layers 1&2 Performance Optimization....57
Background....57
Discovery....58
Preferred NIC Hardware: Intel & Mellanox....60
Don’t Do It: Broadcom & Emulex NICs....61
Mellanox NIC Firmware Updates....62
Watch Out: Non-standard Firewall Interface MTUs....62
Cisco Nexus Interoperability Tips....63
NIC Card Slot Location & Performance....64
A Millisecond in the Life of a Frame....65
The RX “Dark Triad”....67
Network Interface Stability and Error Counters....69
Mitigating Overruns (RX-OVR): Interface Bonding vs. Flow Control....69
Interface Bonding with 802.3ad....70
Special Case: RX-OVR and RX-DRP Increment in Lockstep....73
Beware: Ethernet Flow Control Mechanism (Pause Frames)....73
Other Network Interface Errors: RX-ERR....75
What about RX-DRP?....77
Increasingly Rare but Still Deadly: Duplex Mismatches....77
A Tale of Two Duplexes....80
Firewall Hardware Health Check....81
Firewall Open Hardware BIOS Tuning....83
Spanning Tree Protocol (STP) Sanity Check....84
Layers 1&2 Performance Optimization: Key Points....90

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Chapter 3 Layer 3 Performance Optimization....................91
Background....................91
Discovery & Analysis....................91
The Dual Default Gateway Problem....................92
Asymmetric Path Issue....................96
ICMP Redirect Issue....................100
Special Case: Mismatched Subnet Masks in the Same IP Subnet....................103
Core Router Supernet Loops....................103
ICMP: Canary in the Coal Mine....................105
ARP Neighbor Table Overflows....................106
Layer 3 Performance Optimization: Key Points....................110

Chapter 4 Basic Gaia 3.10 Optimization....................111
Background....................111
Gaia 3.10 Kernel Update....................112
Introduction: User Space Firewall (USFW)....................112
USFW: Discovery....................113
Software Blades Performance Impact....................114
The “top” & “free” Gaia/Linux Commands....................117
Top Output: “us” – Process Space....................117
Top Output: “sy” &”si” – System Space....................121
Top Output: “wa” – Waiting for I/O Operation....................122
Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles....................122
Gaia Memory Management....................123
Firewall Disk Space Check....................124
Solid State Drive (SSD) Considerations....................125
Check Point Specific Commands....................126
Memory Allocation Failures....................126
Connection Table Overflows....................129
Gaia OS Monitoring with cpview....................133
The sar Command....................139
More Granularity Needed? Using top in Batch Mode....................141
Basic Gaia 3.10 Optimization: Key Points....................144

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Chapter 5 ClusterXL HA Performance Tuning............145
Background............145
Make the Call: Where to Focus in this Chapter (or not)............146
Firewall Clustering: High Availability vs. Load Sharing............146
What about VRRP?............149
Performing Administrative Failovers the Right Way............151
Discovery: Cluster Health, State & Interface Status............153
The Magic MAC/Global Cluster ID............156
CCP: Multicast vs. Broadcast vs. Unicast & Interface Flaps............157
Sync Network Health Check............159
Selective Synchronization of Services............162
Troubleshooting “Slow” Failovers............165
Setting Expectations: The ClusterXL Dead Timer............165
The “Cluster Under Load” Mechanism............166
STP and Portfast............166
Dynamic Routing & “Wait for Clustering”............167
Cluster Member Recovery Mode Setting............167
CCP Encryption............169
Q&A: Miscellaneous ClusterXL Topics............169
A Final Option: The ccp_analyzer Tool............171
ClusterXL HA Performance Tuning: Key Points............172

Chapter 6 CoreXL & Multi-Queue............173
Background............173
Discovery............175
Scenario 1: CoreXL on, SecureXL on............177
Scenario 2: CoreXL on, SecureXL off............177
Scenario 3: CoreXL off, SecureXL off............177
Scenario 4: CoreXL off, SecureXL on............178
RX-DRP Analysis & Discussion............179
Network Buffering Misses............180
Special Case: RX-DRP & RX-OVR Increment in Lockstep............182
Remediating Network Buffering Misses (RX-DRP)............183

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

It's a Trap! Increasing Ring Buffer Sizes.............184
Impact of Oversized Ring Buffers – An Example.............186
Seductive but Dangerous: Increase the SoftIRQ Budget.............188
Allocating More CPU Resources for SoftIRQ Processing.............190
Multi-Queue Introduction.............190
Enabled by Default in Gaia 3.10: Multi-Queue.............190
Multi-Queue Parallel Queues Limitations.............192
Process Affinities.............193
Default Core Allocations & CPU Fast Caching.............194
Specific Recommendations by Number of Cores.............196
Special Case: 2 Cores.............198
Special Case: 4 Cores.............200
6-12 Cores Recommendations.............201
16-40 Cores Recommendations.............201
40+ Cores: User Space Firewall (USFW).............201
USFW: Pros and Cons.............202
Adjusting the Firewall Worker Instances: *cpconfig*.............204
Adjusting the Firewall Worker Instances: Gaia Web Interface.............206
RX-DRP Revisited: Still Racking Them Up?.............207
RX-DRP Culprit 1: Unknown or Undesired Protocol Type.............208
RX-DRP Culprit 2: Unexpected or Invalid VLAN Tags.............210
CoreXL Licensing.............212
The Trial License "Core Crunch".............214
The Dynamic Dispatcher.............216
Dynamic Dispatcher Limitations.............216
CoreXL & Multi-Queue: Key Points.............218

Chapter 7 SecureXL Throughput Acceleration & SMT.............219
Background.............219
Discovery.............221
Check for Manual Interface Affinity.............222
SecureXL Introduction.............224
Throughput Acceleration.............226

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

The Processing Paths....226

Accelerated pkts/Total pkts (SXL)....227

F2Fed pkts/Total pkts....227

F2V pkts/Total pkts....228

CPASXL pkts/Total pkts....229

PSLXL pkts/Total pkts....229

QOS inbound & outbound pkts/Total pkts....230

Corrected pkts/Total pkts....230

Big Changes: Comparing SecureXL in R80.10 with R80.20+....230

R80.20+ Core Type Responsibilities....231

SecureXL Packet Flow....234

Accelerated Path Optimization....239

Caution: High Acceleration Rates & SMT/Hyperthreading....239

Discovery: SMT/Hyperthreading....240

Analysis: SMT/Hyperthreading....241

Final Analysis: To SMT or not to SMT....243

Selectively Disabling SecureXL....244

Forcing SecureXL Acceleration with fast_accel....247

Prerequisites For Use of fast_accel and a Warning....247

IP Fragmentation: Nemesis of SecureXL No More....248

SecureXL Tables & Debugging....252

The fwaccel conns Command....253

Processing Path Determination Debugging....254

SecureXL Limitations....256

SecureXL Throughput Acceleration & SMT: Key Points....257

Chapter 8 Access Control Policy Tuning....259

Background....259

Firewall Topology....260

Watch Out: Antispoofing Enforcement....264

The Special Object “Internet”....267

Security Zones....268

Geo Policy & GEO Updatable Objects: Your Secret Weapon....269

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

- Geo Policy vs. GEO Updatable Objects....270
- Performance Comparison: Geo Policy vs. GEO Updatable Objects....274
- Configuring GEO Updatable Objects....274
- Configuring Geo Policy....277
- Case Study: Geo Policy & GEO Objects “Indirect” DNS Blocks....280
- All You Can Eat: Dynamic Block Lists....281

Gateway Performance: Ordered vs. Inline/Unified Layers....282

General Access Control Policy Best Performance Practices....282
- Column-based Matching & Early Drop....283
- “Any” is the Enemy....283

SecureXL Session Rate Acceleration (Accept Templates)....285
- Discovery: SecureXL Accept Templates....286
- SecureXL Accept Templates Background....289
- Policy Tuning to Maximize SecureXL Accept Templating....290
- Other Situations That Can Disable Accept Templating....293

Network Policy Layer Recommendations....294

NAT Policy Optimization....297
- SecureXL NAT Templates....298
- The NAT Cache....300
- The 50K Hide NAT Connection Limit per Destination....303
- Avoiding the Limit: “Many-to-fewer” NAT Configuration....304

APCL/URLF Policy Layer – Cleanup Rules....307

APCL/URLF Best Practices Summary....311
- APCL/URLF Policy: Website Categorization Mode....313

Content Awareness Tips....315

Miscellaneous Policy Optimization & Visibility....316
- Sending a TCP RST upon Connection Expiration....316
- Tracking Connection Timeouts....319
- Logs: Accounting....322
- Your Final Connection-Tracking Option: conn_life_cycle.sh....324

Testing Policies: Packet Mode Searches & fw up_execute....324

Access Control Policy Tuning: Key Points....327

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Chapter 9 Site-To-Site VPN Optimization....329
Introduction & Discovery....329
Make the Call: Where to Focus in this Chapter (or not)....330
MultiCore IPSec VPN & Route-based VPNs....330
3DES vs. AES & AES New Instructions (AES-NI)....331
IPSec VPN Algorithms & SecureXL....332
NAT Traversal (NAT-T)....333
Diffie-Hellman, PFS, & VPN Tunnel Sharing....334
Permanent Tunnels & Dead Peer Detection (DPD)....336
IPSec: Low MTUs & PMTUD....339
Disabling SecureXL Acceleration of IPSec VPN Tunnels....342
Recommended IPSec VPN Settings....345
VPN Limitations....346
Site-To-Site VPN Optimization: Key Points....348

Chapter 10 Threat Prevention Policy Tuning....349
Introduction....349
Quickly Assessing IPS/Threat Prevention Performance Impact....350
Make the Call: Where to Focus in this Chapter (or not)....351
Intrusion Prevention System (IPS) Tuning....352
IPS Basics: The Four “Classes” of IPS Protections....352
IPS Basics: Protection Performance Impact Rankings & Profiles....355
IPS Profile Optimization: IPS ThreatCloud & Core Activations....359
Profile Optimization: Core Activations....362
Profile Optimization: Inspection Settings....362
IPS Profile Optimization: Additional Activation/Deactivation....363
Performance Impact: Inactive vs. Prevent vs. Detect....365
IPS Inspection Coverage: TP Main Layer vs. Legacy “IPS” Layer....366
IPS: Miscellaneous Topics....368
Don’t Even Think About It: IPS Bypass Under Load....368
Avoiding IPS Signatures Known to Disable SecureXL....369
IPS Profiling: Find CPU-hogging IPS Protections....369
Threat Prevention Policy Rule Optimization....370

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Threat Prevention Profile Optimization....................373
General Policy Profile Optimization....................375
Anti-Bot/Anti-Virus Profile Optimization....................380
Threat Emulation/Threat Extraction Profile Optimization....................382
Testing Threat Prevention Policy & Profile Optimizations: CheckMe....................385
PSLXL Path CPU Usage Optimization....................387
Threat Prevention: "Null" Profiles vs. Exceptions....................387
Special Case: Null Profiles vs. Multiple TP Policy Layers....................390
Use Cases for Threat Prevention Exceptions vs. Null Profiles....................390
Special Case: DMZ Networks and Threat Prevention....................392
Threat Prevention Policy Tuning: Key Points....................394

Chapter 11 Active Streaming, Process Space "Trips" & HTTPS Inspection....................395
Background & Discovery....................395
Make the Call: Where to Focus in this Chapter (or not)....................396
Check Point Active Streaming (CPAS)....................396
Security Server Process Space "Trips" & USFW....................397
CPASXL Path Avoidance & Optimization....................401
Security Server Process Space Trips: The List....................404
Special Case: DNS and the rad Daemon....................409
Other rad Daemon Scalability Issues w/ Large User Populations....................411
HTTPS Inspection....................412
HTTPS Inspection Tip: Before We Begin....................414
The Impact: Enabling HTTPS Inspection....................414
HTTPS Inspection Policy Tuning....................415
Other HTTPS Inspection Performance Recommendations....................417
Active Streaming, Process Space "Trips" & HTTPS Inspection: Key Points....................419

Chapter 12 Big Game Hunting: Elephant Flows & DoS Attacks....................421
Background....................421
Elephant Flows: Set Your Priorities & USFW Limitations....................422
Hunting Down Elephant Flows (USFW Disabled)....................424
Diagnosing Elephant Flows (USFW Disabled)....................424
Hunting Down Elephant Flows (USFW Enabled)....................429

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Diagnosing Elephant Flows (USFW Enabled)....429
Remediating Elephant Flows....430
Priority Queues....430
Forcing Acceleration of Elephant Flows with fast_accel....432
SecureXL Rate Limiting & Network Quotas....434
SecureXL and the Quality of Service (QoS) Blade....439
The Hunter Becomes the Hunted: DoS Attacks....440
Aggressive Aging....441
SecureXL and SYN Flood Attacks/Accelerated SYN Defender....443
SecureXL Blacklist....444
Drop Templates & Drop Optimization....445
SecureXL "Penalty Box" Mechanism....448
Management Data Plane Separation....449
Big Game Hunting: Elephant Flows & DoS Attacks Key Points....452

Chapter 13 Intermittent Performance Issues & Setting Proactive Alerts....453
Introduction....453
What Changed & When?....454
Syslog – A Frequently Effective Shortcut....458
Historical Statistics Granularity – cpview vs. sar....459
Running sar and cpview Historical Reports....460
Graphing sar Data – ksar and sadf....462
SmartView Historical Report Graphs....464
Gaia System & Network Checks....467
Check Point Firewall Software Checks....468
Setting Firewall Thresholds & Proactive Alerts....470
First Things First: Types of Alerts and Where to Send Them....471
SmartView Monitor Alerts....472
Aggressive Aging Activation Alert....474
VPN Failure Notifications....475
Cluster Failover Alerts....477
Firewall Low Disk Space Alerts....478
ISP Redundancy – ISP Failure Alert....479

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.

Gaia-based SNMP Traps..480
DiagnosticsView – Troubleshooting Using Only a cpinfo File.................................481
Intermittent Performance Issues & Setting Proactive Alerts: Key Points.................483

Chapter 14 Final Thoughts – The Endless Star..485

Appendix A - Additional Resources & Indexed CLI Quick Reference..........................489
Network/System Commands in Alphabetical Order – Gaia OS & Firewall.............490
Useful tcpdump Filters...510
Network Commands – Cisco IOS..512

LIST OF FIGURES

Figure 1-1: Utilizing CPUSE to Install Jumbo HFAs...35
Figure 1-2: healthcheck.sh Sample Output 1/2..39
Figure 1-3: healthcheck.sh Sample Output 2/2..40
Figure 1-4: Testing Workstation Setup...43
Figure 1-5: Windows *pathping* Command Example...45
Figure 1-6: tc*pdump D*ecode of CDP Traffic..46
Figure 1-7: Wireshark Decode of CDP Traffic..47
Figure 1-8: Invoking SmartView Monitor from the R80+ SmartConsole.........................50
Figure 1-9: Monitoring Blade Additional Reports..51
Figure 1-10: *sar* Command Example..53
Figure 1-11: Using *cpview* to Determine Firewall's Busiest Period.................................54
Figure 2-12: Using *ethtool* to Check NIC Driver Vendors...59
Figure 2-13: Displaying Speed of all Network Interfaces...59
Figure 2-14: Using *ifconfig* to Detect Carrier Transitions..60
Figure 2-15: *netstat -ni* Command Example...68
Figure 2-16: Creating a Bonded Interface...71
Figure 2-17: Bond Transmit Hash Policy..72
Figure 2-18: Using *ethtool -S* to Check Flow Control Counters......................................74

Copyright (c) 2020 Shadow Peak Inc. All Rights Reserved.