



# 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.....                              | 16 |
| 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.....                                          | 24 |
| Beware: Speed Tests & Client-based AntiMalware/AntiVirus Software.....                  | 27 |
| Lab Exercise 1: Explore the Lab, Initial Speed Tests, & CheckMates Community Tools..... | 28 |
| Explore the Current Configuration in the SmartConsole.....                              | 28 |
| Execute Initial Speed Tests and Note Awful Performance.....                             | 30 |
| Work with ccc and s7pac “Super Seven”.....                                              | 32 |
| Module 2 – Network Level Optimization.....                                              | 35 |
| Background.....                                                                         | 35 |
| Latency/Jitter vs. Loss.....                                                            | 35 |
| Measurement & Probing Tools - ping/pathping/mtr/hping/netcat.....                       | 36 |
| Latency/Jitter/Loss - The Impact.....                                                   | 41 |
| New Connection Rates & Rulebase Lookups.....                                            | 41 |
| Measuring Firewall Latency & Application Performance.....                               | 42 |
| IP Fragments Effect on Performance.....                                                 | 44 |
| The RX “Dark Triad”.....                                                                | 46 |
| Network Interface Stability, Error Counters, & Interface Speed Checks.....              | 46 |
| Mitigating Overruns (RX-OVR): Interface Bonding.....                                    | 48 |

|                                                                    |    |
|--------------------------------------------------------------------|----|
| A Common Issue: Bond Traffic Imbalances!.....                      | 48 |
| A Controversial Option: Ethernet Flow Control/Pause Frames.....    | 49 |
| Special Case: RX-OVR and RX-DRP Increment in "Lockstep".....       | 49 |
| Other Network Interface Errors: RX-ERR.....                        | 50 |
| Clearing Network Counters.....                                     | 50 |
| What about RX-DRP?.....                                            | 50 |
| Network Driver Updates – Look Out!.....                            | 50 |
| ARP Neighbor Table Overflows.....                                  | 52 |
| Lab Exercise 2: Diagnose & Correct Network Performance Issues..... | 55 |
| Execute Failover and Run Speed Tests Again.....                    | 55 |
| Fail back Over and Troubleshoot High Latency.....                  | 56 |
| Measure Firewall Latency & Continue Troubleshooting.....           | 57 |
| Troubleshoot Bandwidth Issues.....                                 | 58 |
| Troubleshoot Packet Loss.....                                      | 59 |
| Check Firewall Network Counters.....                               | 59 |
| Correct External Network Issues.....                               | 60 |
| Module 3 – Basic Gaia 3.10/RHEL Optimization.....                  | 66 |
| Background.....                                                    | 66 |
| Gaia Kernel Updates.....                                           | 66 |
| Introduction: User Space Firewall (USFW).....                      | 67 |
| The “top” & “free” Gaia/Linux Commands.....                        | 70 |
| Top Output: “us” & “ni” – Process/User Space.....                  | 71 |
| Top Output: “sy” & “si” – System Space.....                        | 72 |
| Top Output: “wa” – Waiting for I/O Operation.....                  | 72 |
| Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles..... | 73 |
| CPU Usage Spikes: Introducing the Spike Detective.....             | 74 |
| Gaia Memory Management.....                                        | 75 |
| Check Point™ Specific Commands.....                                | 77 |
| Memory Allocation Failures.....                                    | 77 |
| Connection Table Overflows.....                                    | 79 |
| Special Case: Maestro & Connection Table Overflows.....            | 86 |
| HealthCheck Point™ (HCP).....                                      | 87 |

|                                                                                 |            |
|---------------------------------------------------------------------------------|------------|
| HealthCheck Point™ (HCP) "Secret" TAC Tests.....                                | 89         |
| <b>Lab Exercise 3: Examine Gaia Health &amp; Optimize.....</b>                  | <b>90</b>  |
| Run HealthCheck Point™.....                                                     | 90         |
| Run healthcheck.sh.....                                                         | 92         |
| Run Secret Additional "TAC" Tests.....                                          | 92         |
| Unlock & Run "Secret" hcp Performance Reports.....                              | 92         |
| Launch Policy Installation and Observe Waiting for I/O.....                     | 94         |
| Resolve Memory Shortages.....                                                   | 97         |
| Run Speed Tests and Observe Core Utilization.....                               | 100        |
| Launch Port Scan and Observe Connection Table Behavior.....                     | 100        |
| <b>Module 4 – ClusterXL Performance Tuning.....</b>                             | <b>104</b> |
| A Quick Note: SDF and the Correction Layer.....                                 | 104        |
| Sync Network Health Check.....                                                  | 105        |
| Selective Synchronization of Services & Delayed Sync.....                       | 107        |
| Verifying Proper Cluster Operation.....                                         | 110        |
| One More Thing: The "Cluster Under Load" Mechanism.....                         | 110        |
| <b>Lab Exercise 4: Verify Cluster Operation &amp; Sync Network Health.....</b>  | <b>111</b> |
| Checking Cluster Status.....                                                    | 111        |
| Cause a Catastrophic Failover and Observe Behavior.....                         | 111        |
| Cause a Non-Catastrophic Failover and Observe Behavior.....                     | 114        |
| Check & Correct Sync Network Health.....                                        | 114        |
| Verify the Default Setting for Delayed Sync.....                                | 117        |
| <b>Module 5 – CoreXL &amp; Multi-Queue.....</b>                                 | <b>118</b> |
| Old School <R81: CoreXL "Static Split".....                                     | 119        |
| New School R81+: CoreXL Dynamic Balancing ("Dynamic Split").....                | 121        |
| RX-DRP & Ring Buffer Sizes.....                                                 | 126        |
| Multi-Queue Introduction.....                                                   | 128        |
| Multi-Queue Parallel Queues Limitations.....                                    | 128        |
| The Dynamic Dispatcher & Priority Queueing.....                                 | 131        |
| SND/IRQ Core Balancing.....                                                     | 133        |
| Tracking Down Unexplained High CPU Usage: The Undocumented "perf" Command.....  | 135        |
| Troubleshooting Persistent, Excessive CPU Utilization on a Particular Core..... | 136        |

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| CoreXL Frontiers: Intel's "P-Cores"/"E-Cores" .....                                    | 139 |
| Lab Exercise 5: Multi-Queue, CoreXL Splits, and Static CoreXL Split Changes.....       | 140 |
| Examine Multi-Queue Configuration.....                                                 | 140 |
| Correct Multi-Queue & Ring Buffer Issues.....                                          | 141 |
| Work with the Dynamic Dispatcher/Priority Queues & Enable.....                         | 142 |
| Modifying the Static CoreXL Split.....                                                 | 145 |
| Module 6 – SecureXL Throughput Acceleration.....                                       | 149 |
| SecureXL Introduction Part 1 - Throughput Acceleration.....                            | 149 |
| SecureXL Introduction Part 2 – Accept Templates.....                                   | 150 |
| Throughput Acceleration – fwaccel stats -s.....                                        | 152 |
| Accelerated conns/Total conns (Software Accept Template Match).....                    | 153 |
| LightSpeed conns/Total Conns (Hardware Accept Template Match).....                     | 153 |
| Accelerated pkts/Total pkts (Software Fastpath).....                                   | 153 |
| LightSpeed pkts/Total pkts (Hardware Fastpath).....                                    | 153 |
| F2Fed pkts/Total pkts.....                                                             | 153 |
| F2V pkts/Total pkts.....                                                               | 154 |
| CPASXL pkts/Total pkts.....                                                            | 154 |
| PSLXL pkts/Total pkts.....                                                             | 154 |
| CPAS Pipeline & PSL Pipeline.....                                                      | 155 |
| UDP IS XL pkts/Total pkts & UDP IS pipeline pkts/Total pkts (R82+ only).....           | 155 |
| QOS inbound & outbound pkts/Total pkts.....                                            | 155 |
| Corrected pkts/Total pkts.....                                                         | 155 |
| Core Type Responsibilities & Relative Process Path Efficiency.....                     | 155 |
| Path Optimization Strategy.....                                                        | 158 |
| Corner Case: High Acceleration Rates & SMT/Hyperthreading.....                         | 159 |
| Selectively Disabling SecureXL.....                                                    | 159 |
| Forcing SecureXL Acceleration with fast_accel.....                                     | 161 |
| The "fwaccel conns", "fw_mux all", fw_streaming, & "fw ctl multik gconn" Commands..... | 164 |
| Processing Path Determination Techniques.....                                          | 166 |
| The Easy Way: "fw tab -t connections -z" .....                                         | 166 |
| The Hard Way: Performing a Kernel Debug.....                                           | 166 |
| SecureXL Throughput Acceleration Limitations.....                                      | 167 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| SecureXL Frontiers: LightSpeed, UPPAK, & R82's Parallel Processing Flows.....                    | 169 |
| Lab Exercise 6: Observing SecureXL Behavior & Determining Why Traffic is F2F.....                | 173 |
| Examine Throughput Acceleration Levels.....                                                      | 173 |
| Execute Debug to Determine Why Certain Traffic is F2F/slowpath.....                              | 176 |
| Remove Manual F2F Definition.....                                                                | 178 |
| Set Up & Test Fast_Accel.....                                                                    | 181 |
| Module 7 – Access Control Policy Tuning.....                                                     | 183 |
| Background.....                                                                                  | 183 |
| The Importance of a Properly Defined Firewall Topology.....                                      | 183 |
| The Special Policy Object “Internet” & APCL/URLF Rules.....                                      | 187 |
| rad Daemon Scalability Issues with Large User Populations.....                                   | 190 |
| Access Control Rules: Column-based Matching.....                                                 | 192 |
| Beware: Use of Domain Objects and Wildcards in Custom Application/Site Objects.....              | 192 |
| SecureXL Session Rate Acceleration (Accept Templates).....                                       | 195 |
| The Few Services & Rulebase Conditions That Can Still Disable Accept Templating in R80.10+ ..... | 197 |
| But Wait, the Actual Accept Templating Rate is Always Zero?.....                                 | 198 |
| Cause #1: Enabling More Blades Than Just "Firewall" in the Top/Parent Policy Layer.....          | 198 |
| Cause #2: Use of "Protocol Signature" Option on Service Objects.....                             | 200 |
| Zero Accept Template Rate Diagnosis: fwaccel templates -R.....                                   | 202 |
| SecureXL Drop Templates and the Penalty Box.....                                                 | 203 |
| NAT Policy Optimization.....                                                                     | 205 |
| IPSec VPN Performance Tuning.....                                                                | 208 |
| VPNs: 3DES vs. AES & AES New Instructions (AES-NI) & GCM.....                                    | 208 |
| VPNs: IPSec: Low MTUs & PMTUD.....                                                               | 211 |
| IGB/IXGBE/ICE Driver Issues Balancing IPSec Traffic on SNDs.....                                 | 213 |
| Lab Exercise 7: Object Internet, Accept Templates, Optimizing APCL/URLF Policies.....            | 214 |
| APCL/URLF Policy Optimization.....                                                               | 214 |
| Optimize SecureXL Accept Templates.....                                                          | 218 |
| Configure & Test the SecureXL Penalty Box.....                                                   | 222 |
| VPN Optimization Exercise.....                                                                   | 225 |
| Module 8 – Threat Prevention Policy Tuning.....                                                  | 229 |

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| Introduction.....                                                            | 229 |
| Quickly Assessing IPS/Threat Prevention Performance Impact.....              | 229 |
| IPS Inspection Coverage: TP Main Layer vs. Legacy “IPS” Layer.....           | 231 |
| Cut to the Chase: hcp’s “Secret” TP Reports.....                             | 233 |
| IPS Bypass Under Load: Formerly Unusable But Now an Option.....              | 235 |
| Performance Impact: Inactive vs. Prevent vs. Detect.....                     | 236 |
| Custom IPS Profile Optimization: IPS ThreatCloud & Core Activations.....     | 236 |
| Custom Profile Optimization: Inspection Settings.....                        | 238 |
| Performance: IPS Blade vs. Anti-Virus.....                                   | 239 |
| Threat Prevention: “Null” Profiles vs. Blade-based Exceptions.....           | 243 |
| Threat Prevention Blade-Based Exceptions.....                                | 244 |
| Threat Prevention “Null Profiles”.....                                       | 247 |
| Custom vs. Autonomous TP Policy Management.....                              | 248 |
| Lab Exercise 8: Finding F2F TP traffic, hcp, & Blade-based Exceptions.....   | 249 |
| Diagnosing Threat Prevention Performance Issues.....                         | 249 |
| Disable Threat Prevention and Retest Performance.....                        | 250 |
| Run “Secret” hcp Threat Prevention Performance Reports.....                  | 251 |
| Examine SmartConsole Threat Prevention Configuration.....                    | 253 |
| Engage TP Profile Cleanup Options.....                                       | 254 |
| Retest Performance after Optimizations.....                                  | 256 |
| Create Blade-based Exception & Retest Speed.....                             | 259 |
| Module 9 – HTTPS Inspection Optimization.....                                | 264 |
| The Impact: Enabling HTTPS Inspection.....                                   | 264 |
| Quick Mention: Outbound “Lite” Inspection a.k.a. Categorize HTTPS Sites..... | 264 |
| HTTPS Inspection Policy Optimization Best Practices.....                     | 266 |
| HTTPS Inspection Policy Tips & Tricks.....                                   | 268 |
| HTTPS Inspection Performance Tips & Tricks.....                              | 269 |
| HTTPS Inspection Frontiers in R82+.....                                      | 270 |
| Lab Exercise 9: Optimize an HTTPS Inspection Policy (Optional).....          | 271 |
| Identify Active Streaming Connections.....                                   | 271 |

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Optimize Existing HTTPS Inspection Policy to Best Practices.....                        | 273 |
| Retest Active Streaming Performance After Optimizations.....                            | 280 |
| Verify HTTPS Inspection Policy Operation.....                                           | 282 |
| Module 10 – Heavy Connections/Elephant Flows & HyperFlow/Pipeline Processing.....       | 284 |
| Identifying Elephant/Heavy Connections.....                                             | 284 |
| Remediating Elephant Flows.....                                                         | 286 |
| SecureXL Rate Limiting & Network Quotas.....                                            | 287 |
| SecureXL and the Quality of Service (QoS) Blade.....                                    | 288 |
| R81.20: HyperFlow & the "Pipeline" SecureXL Paths.....                                  | 288 |
| HyperFlow Example.....                                                                  | 292 |
| Monitoring/Configuring HyperFlow – CLI Commands.....                                    | 295 |
| Monitoring HyperFlow – cpview.....                                                      | 296 |
| Monitoring HyperFlow – SmartConsole.....                                                | 299 |
| Lab Exercise 10: Heavy Connections, Dynamic Split & HyperFlow.....                      | 300 |
| Create Multiple Elephant Flows & View Statistics.....                                   | 300 |
| Enable Dynamic Balancing/Split & Hyperflow.....                                         | 302 |
| Test Dynamic Split.....                                                                 | 303 |
| Test HyperFlow/Pipeline Processing.....                                                 | 307 |
| Enforce Rate Limits.....                                                                | 313 |
| Appendix A – Intermittent/Historical Performance Issues Investigation & Monitoring..... | 316 |
| Syslog – A Frequently Effective Shortcut.....                                           | 316 |
| cpview History Mode.....                                                                | 317 |
| Getting A “Second Opinion” - The sar Command.....                                       | 318 |
| New Monitoring Frontiers – Skyline.....                                                 | 322 |
| Check the Spike Detective.....                                                          | 323 |
| What Else Changed?.....                                                                 | 323 |
| SmartView Monitor Reports.....                                                          | 324 |
| Optional Lab: cpview History Mode & the sar Command.....                                | 325 |
| cpview Historical Mode.....                                                             | 326 |
| Getting a “Second Opinion” from the CLI with sar.....                                   | 326 |

Appendix B – Maestro/Scalable Platforms Commands.....328

    Live Performance Overview: asg perf -vp.....329

    Finding Performance "Hogs": asg\_perf\_hogs.....331

    Diagnostics for Scalable Platforms/Maestro: asg diag.....332

    Setting Limits with Session Control Rules: asg\_session\_control.....333

    Finding Which SGM (and path) is Handling a Degraded Connection: asg search.....334

    Packet Distribution Issues Between SGM’s: show distribution.....335

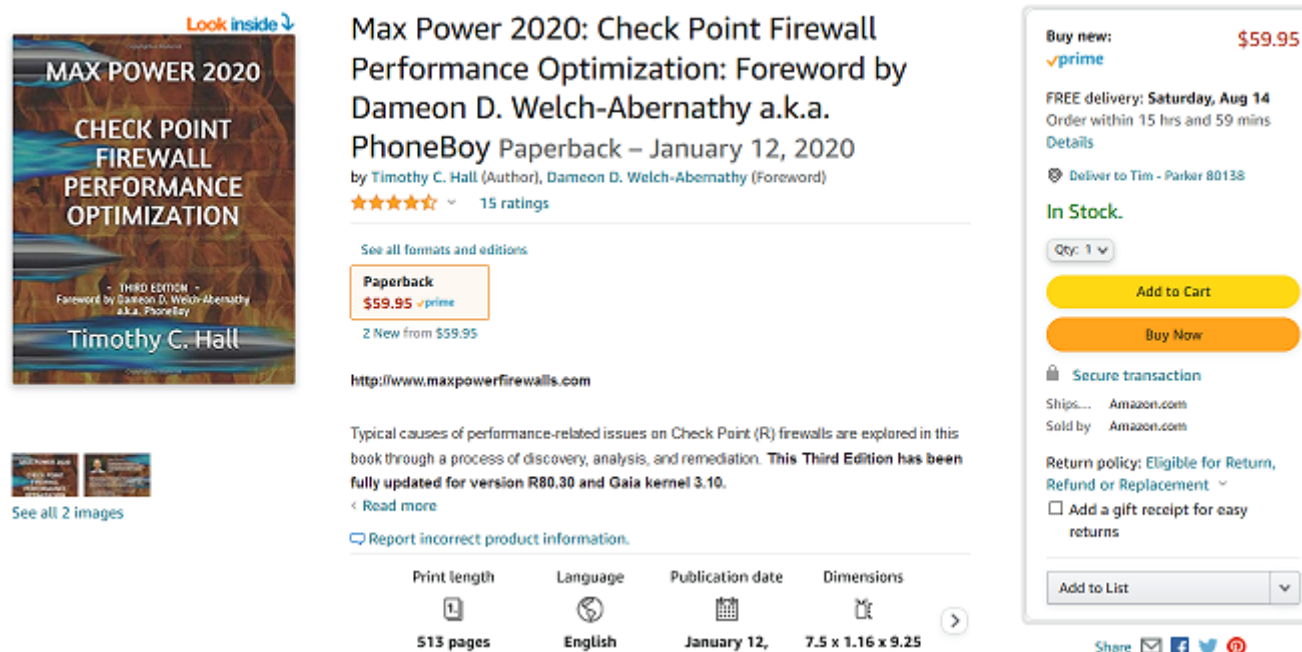
Appendix C: GEO Updatable Objects - Your Secret Performance Weapon.....336

    Geo Policy vs. GEO Updatable Objects.....337

Wrap–up Discussion and Additional Resources.....339

# 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](#) (3,700+), [Link to all CPUG.org posts](#) (2,200+)
  - Author of the Book “Max Power 2020: Check Point™ Firewall Performance Optimization”



The image shows an Amazon product page for the book "Max Power 2020: Check Point Firewall Performance Optimization" by Timothy C. Hall. The book cover is visible on the left, showing the title and author. The main text area provides details about the book, including the foreword by Dameon D. Welch-Abernathy, the publication date (January 12, 2020), and the author's name. The price is listed as \$59.95, with a Prime discount. The page also includes a "Look inside" link, a "See all formats and editions" link, and a "Report incorrect product information" link. The right sidebar shows the "Buy new" price, delivery information, and buttons for "Add to Cart" and "Buy Now".

**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 from 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 of experience working with Check Point™ gateways in a production environment. Preferred: Minimum 5 years of experience working with Check Point™ gateways in 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™.
- The latest performance-related features for version R82 are covered in the lecture segments only.
- Your lab exercises are in a break/fix format. Many issues and badly-optimized configurations based on real-world problems were introduced to your lab environment before 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 primary 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 fully covered, but will be mentioned a number of times with linked references provided for further reading. 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 crafted explicitly 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