



Gateway Performance Optimization

Timothy C. Hall, Shadow Peak Inc.



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

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.....	67
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.....	70
Firewall Hardware Health Check & Weird CPU Usage.....	71
Gaia Memory Management.....	72
Check Point™ Specific Commands.....	73
Memory Allocation Failures.....	73
Connection Table Overflows.....	75
A “Second Opinion” - The sar Command.....	79
HealthCheck Point™ (HCP).....	81

Lab Exercise 3: Examine Gaia Health & Optimize.....	83
Run HealthCheck Point™.....	83
Run healthcheck.sh.....	85
Unlock & Run "Secret" hcp Performance Reports.....	85
Run Speed Tests and Observe Core Utilization.....	87
Launch Port Scan and Observe Connection Table Behavior.....	87
Launch Policy Installation and Observe Waiting for I/O.....	90
Resolve Memory Shortages.....	93
Module 4 – ClusterXL Performance Tuning.....	97
A Quick Note: SDF and the Correction Layer.....	97
Sync Network Health Check.....	97
Selective Synchronization of Services & Delayed Sync.....	99
Verifying Proper Cluster Operation.....	102
Lab Exercise 4: Verify Cluster Operation & Sync Network Health.....	103
Checking Cluster Status.....	103
Cause a Catastrophic Failover and Observe Behavior.....	103
Cause a Non-Catastrophic Failover and Observe Behavior.....	106
Check & Correct Sync Network Health.....	106
Verify the Default Setting for Delayed Sync.....	109
Module 5 – CoreXL & Multi-Queue.....	110
Old School <R81: CoreXL "Static Split".....	110
New School R81+: CoreXL Dynamic Balancing ("Dynamic Split").....	112
RX-DRP & Ring Buffer Sizes.....	116
Multi-Queue Introduction.....	117
Multi-Queue Parallel Queues Limitations.....	117
The Dynamic Dispatcher & Priority Queueing.....	119
SND/IRQ Core Balancing.....	122
Lab Exercise 5: Multi-Queue, CoreXL Splits, and Static CoreXL Split Changes.....	124
Examine Multi-Queue Configuration.....	124
Correct Multi-Queue & Ring Buffer Issues.....	125
Work with the Dynamic Dispatcher/Priority Queues & Enable.....	126

Modifying the Static CoreXL Split.....	130
Module 6 – SecureXL Throughput Acceleration.....	134
SecureXL Introduction Part 1 - Throughput Acceleration.....	134
SecureXL Introduction Part 2 – Accept Templates.....	135
Throughput Acceleration – fwaccel stats -s.....	136
Accelerated conns/Total conns.....	137
LightSpeed conns/Total Conns.....	137
Accelerated pkts/Total pkts (Software Fastpath).....	137
LightSpeed pkts/Total pkts (Hardware Fastpath).....	137
F2Fed pkts/Total pkts.....	137
F2V pkts/Total pkts.....	138
CPASXL pkts/Total pkts.....	138
PSLXL pkts/Total pkts.....	138
CPAS Pipeline & PSL Pipeline.....	138
QOS inbound & outbound pkts/Total pkts.....	139
Corrected pkts/Total pkts.....	139
Core Type Responsibilities & Relative Process Path Efficiency.....	139
Path Optimization Strategy.....	140
Corner Case: High Acceleration Rates & SMT/Hyperthreading.....	141
Selectively Disabling SecureXL.....	142
Forcing SecureXL Acceleration with fast_accel.....	143
The "fwaccel conns", "fw_mux all", fw_streaming, & "fw ctl multik gconn" Commands.....	146
Processing Path Determination Debugging.....	146
SecureXL Throughput Acceleration Limitations.....	148
New SecureXL Frontiers: LightSpeed & UPPAK.....	149
Lab Exercise 6: Observing SecureXL Behavior & Determining Why Traffic is F2F.....	150
Examine Throughput Acceleration Levels.....	150
Execute Debug to Determine Why Certain Traffic is F2F/slowpath.....	153
Remove Manual F2F Definition.....	155
Set Up Fast_Accel.....	159
Module 7 – Access Control Policy Tuning.....	161

Background.....	161
The Importance of a Properly Defined Firewall Topology.....	161
The Special Policy Object “Internet” & APCL/URLF Rules.....	164
GEO Updatable Objects: Your Secret Performance Weapon.....	167
Geo Policy vs. GEO Updatable Objects.....	168
rad Daemon Scalability Issues w/ Large User Populations.....	169
Access Control Column-based Matching: “Any” is the Enemy.....	171
Beware: Use of Domain Objects.....	173
SecureXL Session Rate Acceleration (Accept Templates).....	173
The Few Services & Rulebase Conditions That Can Still Disable Accept Templating in R80.10+.....	175
SecureXL Drop Templates and the Penalty Box.....	178
NAT Policy Optimization.....	180
IPSec Site-To-Site VPN Performance Tuning.....	181
VPNs: 3DES vs. AES & AES New Instructions (AES-NI).....	181
IPSec VPN Recommended Algorithms.....	182
VPNs: IPSec: Low MTUs & PMTUD.....	183
Lab Exercise 7: Object Internet, Accept Templates, Optimizing APCL/URLF Policies.....	186
APCL/URLF Policy Optimization.....	186
Optimize SecureXL Accept Templates.....	190
Configure & Test the SecureXL Penalty Box.....	193
NAT Optimization Exercise.....	197
VPN Optimization Exercise.....	200
Module 8 – Threat Prevention Policy Tuning.....	204
Introduction.....	204
Quickly Assessing IPS/Threat Prevention Performance Impact.....	204
IPS Inspection Coverage: TP Main Layer vs. Legacy “IPS” Layer.....	206
Cut to the Chase: hcp’s Secret TP Reports.....	207
Don’t Even Think About It: IPS Bypass Under Load.....	210
Performance Impact: Inactive vs. Prevent vs. Detect.....	210
Custom IPS Profile Optimization: IPS ThreatCloud & Core Activations.....	211

Custom Profile Optimization: Inspection Settings.....	213
Threat Prevention: “Null” Profiles vs. Blade-based Exceptions.....	213
Threat Prevention Blade-Based Exceptions.....	215
Threat Prevention "Null Profiles"	218
Custom vs. Autonomous TP Policy Management.....	220
Lab Exercise 8: Finding F2F TP traffic, Exceptions & Null Profiles.....	221
Diagnosing Threat Prevention Performance Issues.....	221
Disable Threat Prevention and Retest Performance.....	222
Run "Secret" hcp Threat Prevention Performance Reports.....	223
Examine SmartConsole Threat Prevention Configuration.....	226
Engage TP Profile Cleanup Options.....	227
Retest Performance after Optimizations.....	229
Create Blade-based Exception & Retest Speed.....	232
Module 9 – HTTPS Inspection Optimization.....	237
The Impact: Enabling HTTPS Inspection.....	237
Quick Mention: Outbound "Lite" Inspection a.k.a. Categorize HTTPS Sites.....	237
HTTPS Inspection Policy Optimization Best Practices.....	239
Lab Exercise 9: Optimize an HTTPS Inspection Policy.....	243
Identify Active Streaming Connections.....	243
Optimize Existing HTTPS Inspection Policy to Best Practices.....	245
Retest Active Streaming Performance After Optimizations.....	251
Verify HTTPS Inspection Policy Operation.....	253
Module 10 – Heavy Connections/Elephant Flows & HyperFlow/Pipeline Processing.....	255
Identifying Elephant/Heavy Connections.....	255
Remediating Elephant Flows.....	256
SecureXL Rate Limiting & Network Quotas.....	257
SecureXL and the Quality of Service (QoS) Blade.....	258
R81.20: HyperFlow & the "Pipeline" SecureXL Paths.....	258
HyperFlow Example.....	262
Monitoring/Configuring HyperFlow – CLI Commands.....	265

Monitoring HyperFlow – cpview.....	267
Monitoring HyperFlow – SmartConsole.....	270
Lab Exercise 10: Heavy Connections, Dynamic Split & HyperFlow.....	271
Create Multiple Elephant Flows & View Statistics.....	271
Enable Dynamic Balancing/Split & Hyperflow.....	273
Test Dynamic Split.....	274
Test HyperFlow/Pipeline Processing.....	278
Enforce Rate Limits.....	284
Appendix A – Intermittent/Historical Performance Issues Investigation & Monitoring.....	287
Syslog – A Frequently Effective Shortcut.....	287
cpview History Mode.....	288
New Monitoring Frontiers – Skyline.....	289
Getting a "Second Opinion": The sar Command.....	291
Check the Spike Detective.....	292
What Else Changed?.....	292
SmartView Monitor Reports.....	292
Optional Lab: cpview History Mode & the sar Command.....	293
cpview Historical Mode.....	294
Getting a “Second Opinion” from the CLI with sar.....	294
Appendix B – Maestro/Scalable Platforms Commands.....	296
Live Performance Overview: asg perf -vp.....	296
Finding Performance "Hogs": asg_perf_hogs.....	298
Diagnostics for Scalable Platforms/Maestro: asg diag.....	299
Setting Limits with Session Control Rules: asg_session_control.....	300
Finding Which SGM (and path) is Handling a Degraded Connection: asg search.....	301
Packet Distribution Issues Between SGM’s: show distribution.....	302
Wrap-up Discussion and Additional Resources.....	303