MAX POWER

Check Point Firewall

Performance Optimization
# TABLE OF CONTENTS

List of Figures vii  
List of Tables xi  

Foreword by Dameon D. Welch-Abernathy xiii  

Preface xv  
  Why was this book created? xv  
  How to use this book xvi  
  Conventions xvii  
  And Now for a Word xix  
  About the Author xx  

Acknowledgements xxiii  

Chapter 1 Introduction & Concepts 1  
  Introduction 1  
  Background: Check Point History & Architecture 2  
  Methodology 3  
  Latency vs. Loss 3  
  Test Environment Setup 4  
  A Millisecond in the Life of a Frame 6  
  Discovery 9  
  The RX “Dark Triad” 14  
  Monitoring Blade Present? 15  
  Introduction & Concepts: Key Points 17  

Chapter 2 Layer 1 Performance Optimization 19  
  Background 19  
  Discovery & Analysis 20  
  Layer 1 Performance Optimization: Key Points 32
## Table of Contents

Chapter 3 Layers 2 & 3 Performance Optimization 33
  - Background 33
  - Discovery & Analysis 35
  - Special Case: The Dual Default Gateway Problem 39
    - Asymmetric Path Issue 42
    - ICMP Redirect Issue 46
  - ARP Neighbor Table Overflows 50
  - Layers 2 & 3 Performance Optimization: Key Points 54

Chapter 4 Gaia & Basic Check Point Optimization 55
  - Background 55
  - Discovery and Analysis 56
    - Software Blades Performance Impact 56
    - The top, free, and df Gaia/Linux Commands 58
    - Check Point Specific Commands 65
  - Intermittent Performance Issues 72
    - Sar Command and Using top in Batch Mode 73
    - Virtual Links 77
    - Firewall Gateway Thresholds 83
  - Firewall Security Policy Best Performance Practices 84
    - Sending a TCP RST upon Connection Expiration 87
    - Enhanced Logging of Connection Timeouts 90
    - Firewall Cluster-Specific Performance Issues 91
      - Selective Synchronization of Services 92
    - Firewall Clustering: High Availability vs. Load Sharing 99
  - Gaia & Basic Check Point Optimization: Key Points 102

Chapter 5 CoreXL Tuning 105
  - Background 105
  - Discovery & Analysis 108
    - Scenario 1: CoreXL on, SecureXL on 109
    - Scenario 2: CoreXL on, SecureXL off 110
    - Scenario 3: CoreXL off, SecureXL off 110
    - Scenario 4: CoreXL off, SecureXL on 111
  - RX-DRP Analysis & Discussion 112
    - Network Buffering Misses 114
    - Remediating Network Buffering Misses 116
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact of Oversized Ring Buffers – An Example</td>
<td>118</td>
</tr>
<tr>
<td>More CPU Resources for SoftIRQ Needed?</td>
<td>120</td>
</tr>
<tr>
<td>Default Core Allocations &amp; CPU Fast Caching</td>
<td>123</td>
</tr>
<tr>
<td>Specific Recommendations by Number of Cores</td>
<td>124</td>
</tr>
<tr>
<td>Special Case: 2 Cores</td>
<td>127</td>
</tr>
<tr>
<td>4 cores</td>
<td>129</td>
</tr>
<tr>
<td>6 cores</td>
<td>131</td>
</tr>
<tr>
<td>8 cores</td>
<td>132</td>
</tr>
<tr>
<td>12 cores</td>
<td>133</td>
</tr>
<tr>
<td>16 cores</td>
<td>134</td>
</tr>
<tr>
<td>20 cores</td>
<td>135</td>
</tr>
<tr>
<td>24 cores</td>
<td>136</td>
</tr>
<tr>
<td>Adjusting the Number of Firewall Worker Cores</td>
<td>136</td>
</tr>
<tr>
<td>CoreXL Licensing</td>
<td>139</td>
</tr>
<tr>
<td>CoreXL and VPN Performance</td>
<td>141</td>
</tr>
<tr>
<td>MultiCore SSL</td>
<td>142</td>
</tr>
<tr>
<td>3DES vs AES and AES NI</td>
<td>143</td>
</tr>
<tr>
<td>CoreXL IPSec VPN Single-Core Tasking</td>
<td>144</td>
</tr>
<tr>
<td>Low MTUs and PMTUD</td>
<td>146</td>
</tr>
<tr>
<td>CoreXL Unsupported VPN Features</td>
<td>148</td>
</tr>
<tr>
<td>CoreXL Firewall Worker Load Distribution</td>
<td>149</td>
</tr>
<tr>
<td>RX-DRP Revisited: Still Racking Them Up?</td>
<td>151</td>
</tr>
<tr>
<td>RX-DRP Culprit 1: Unknown or Undesired Protocol Type</td>
<td>152</td>
</tr>
<tr>
<td>RX-DRP Culprit 2: Unexpected or Invalid VLAN Tags</td>
<td>154</td>
</tr>
<tr>
<td>CoreXL Tuning: Key Points</td>
<td>157</td>
</tr>
<tr>
<td>Chapter 6 SecureXL Throughput Acceleration</td>
<td>159</td>
</tr>
<tr>
<td>Background</td>
<td>159</td>
</tr>
<tr>
<td>SecureXL Introduction</td>
<td>164</td>
</tr>
<tr>
<td>Throughput Acceleration</td>
<td>165</td>
</tr>
<tr>
<td>Packet/Throughput Acceleration Tuning</td>
<td>169</td>
</tr>
<tr>
<td>Accelerated Path Optimization</td>
<td>174</td>
</tr>
<tr>
<td>IPS Protection Scope Setting</td>
<td>176</td>
</tr>
<tr>
<td>Signature Performance Impact Rankings</td>
<td>179</td>
</tr>
<tr>
<td>Avoiding IPS Signatures Known to Disable Throughput Acceleration</td>
<td>182</td>
</tr>
<tr>
<td>APCL/URLF Accelerated Path Optimization</td>
<td>183</td>
</tr>
<tr>
<td>APCL/URLF Topology &amp; Internet Object Issues</td>
<td>184</td>
</tr>
</tbody>
</table>
# Table of Contents

## Chapter 7 SecureXL Session Rate Acceleration
- Background
- Discovery
- Session Rate Acceleration Security Policy Tuning
- Other Situations That Can Disable Session Acceleration
- NAT Templates & the NAT Cache Table
- Drop Templates & Drop Optimization
- Increasing Resistance to Denial of Service Attacks
  - IPS Aggressive Aging
  - Firewall Enhanced Durability/Heavy Load QoS
  - SecureXL “Penalty Box” Mechanism
- Rate Limiting for DDoS Mitigation/Network Quota
- SecureXL Session Rate Acceleration: Key Points

## Chapter 8 Multi-Queue & Hyperspect
- Background
- Discovery: Multi-Queue

---

**APCL/URLF Policy Source Optimization** 186  
**APCL/URLF Policy Service Optimization** 189  
**APCL/URLF Policy “Cleanup Rule”** 191  
**Threat Prevention Optimization** 193  
**Medium Path CPU Usage Optimization** 194  
**Creating IPS Exceptions** 195  
**IPS Exceptions: Semi-Trusted & Non-Trusted Internet Sites** 199  
**IPS Exceptions: Intra-DMZ Interaction & DMZ Backend Connections** 201  
**IPS Exceptions: Internal to DMZ Connections** 203  
**IPS Exceptions: Traffic between Trusted Internal Networks** 204  
**Special Case: IPS Engine Settings Known to Eat CPU** 204  
**IPS Profiling: Find CPU-Hogging IPS Protections** 208  
**APCL/URLF Policy Website Categorization Mode** 211  
**APCL/URLF Logging Optimization** 213  
**Firewall Path Optimization** 215  
**IP Fragmentation: Nemesis of SecureXL** 216  
**HTTPS Inspection Feature** 220  
**Which Path is a Certain Connection Using, and Why?** 221  
**SecureXL Throughput Acceleration: Key Points** 226  

Copyright © 2015 Shadow Peak Inc. All rights reserved.
maxpowerfirewalls.com
## Table of Contents

<table>
<thead>
<tr>
<th>Chapter 9 Manual Affinity</th>
<th>281</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>281</td>
</tr>
<tr>
<td>Scenario 1: Lab Benchmark</td>
<td>282</td>
</tr>
<tr>
<td>Scenario 2: Firewall Moderately Overloaded</td>
<td>282</td>
</tr>
<tr>
<td>Scenario 3: Firewall Severely Overloaded</td>
<td>283</td>
</tr>
<tr>
<td>Discovery</td>
<td>285</td>
</tr>
<tr>
<td>Manual Affinities &amp; SecureXL</td>
<td>286</td>
</tr>
<tr>
<td>Manual Interface Affinity with SecureXL Enabled</td>
<td>286</td>
</tr>
<tr>
<td>Manual Interface Affinity with SecureXL Disabled</td>
<td>289</td>
</tr>
<tr>
<td>Manual Daemon Process &amp; Kernel Affinity</td>
<td>291</td>
</tr>
<tr>
<td>Atrocious Affinity Archetype</td>
<td>294</td>
</tr>
<tr>
<td>Manual Affinity: Key Points</td>
<td>297</td>
</tr>
</tbody>
</table>

| Chapter 10 Final Thoughts - Rinse and Repeat | 299 |

<table>
<thead>
<tr>
<th>Indexed CLI Quick Reference</th>
<th>301</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network/System Commands – Gaia/Linux OS</td>
<td>302</td>
</tr>
<tr>
<td>Useful Tcpdump Filters</td>
<td>308</td>
</tr>
<tr>
<td>Check Point General System Commands</td>
<td>309</td>
</tr>
<tr>
<td>Check Point CoreXL/SecureXL Commands</td>
<td>312</td>
</tr>
<tr>
<td>Hyperspect/Multi-Queue Commands</td>
<td>316</td>
</tr>
<tr>
<td>Manual Affinity Commands</td>
<td>317</td>
</tr>
<tr>
<td>Network Discovery Commands – Cisco IOS</td>
<td>318</td>
</tr>
</tbody>
</table>