

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

ii 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

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

iv Table of Contents

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
 Chapter 7 SecureXL Session Rate Acceleration	 229
Background	229
Discovery	234
Session Rate Acceleration Security Policy Tuning	238
Other Situations That Can Disable Session Acceleration	244
NAT Templates & the NAT Cache Table	245
Drop Templates & Drop Optimization	249
Increasing Resistance to Denial of Service Attacks	254
IPS Aggressive Aging	254
Firewall Enhanced Durability/Heavy Load QoS	257
SecureXL “Penalty Box” Mechanism	257
Rate Limiting for DDoS Mitigation/Network Quota	258
SecureXL Session Rate Acceleration: Key Points	263
 Chapter 8 Multi-Queue & Hyperspect	 265
Background	265
Discovery: Multi-Queue	267

Analysis: Multi-Queue	268
Multi-Queue: RX-DRP Still Incrementing Regularly?	273
Discovery: Hyperspect	273
Analysis: Hyperspect	277
Special Case: IPSec VPNs & Hyperspect	278
Multi-Queue & Hyperspect: Key Points	279
 Chapter 9 Manual Affinity	 281
Background	281
Scenario 1: Lab Benchmarking	282
Scenario 2: Firewall Moderately Overloaded	282
Scenario 3: Firewall Severely Overloaded	283
Discovery	285
Manual Affinities & SecureXL	286
Manual Interface Affinity with SecureXL Enabled	286
Manual Interface Affinity with SecureXL Disabled	289
Manual Daemon Process & Kernel Affinity	291
Atrocious Affinity Archetype	294
Manual Affinity: Key Points	297
 Chapter 10 Final Thoughts - Rinse and Repeat	 299
 Indexed CLI Quick Reference	 301
Network/System Commands – Gaia/Linux OS	302
Useful Tcpdump Filters	308
Check Point General System Commands	309
Check Point CoreXL/SecureXL Commands	312
Hyperspect/Multi-Queue Commands	316
Manual Affinity Commands	317
Network Discovery Commands – Cisco IOS	318