

Gaia 4.18 (R82) Immersion: Tips, Tricks, & Best Practices



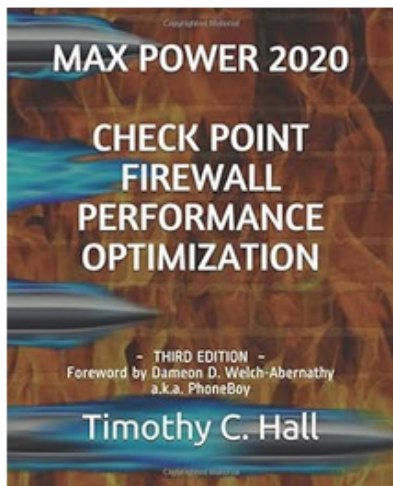
Shadow Peak

SECURITY TRAINING AND SERVICES

Welcome & Introduction

- Your Instructor: **Timothy Hall, CISSP**
 - Worked with Check Point products since 1997, Check Point certified instructor since 2004
 - Founder of Shadow Peak Inc, a Check Point Authorized Training Center (ATC) (<https://www.shadowpeak.com>)
 - [Link to 3,800+ CheckMates Posts](#) [Link to 2,200+ CPUG Posts](#) Also the author of book “Max Power 2020: Check Point Firewall Performance Optimization”

Books › Computers & Technology › Programming › Software Design, Testing & Engineering › Performance Optimization



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)

4.6 ★★★★★ 22 ratings

<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.**



☐ Add Prime to get **Fast, Free delivery**



Paperback
\$69.95

Other Used and New from \$30.95 ▼

Buy new:

\$69⁹⁵

FREE Returns ▼

FREE delivery **Sunday, June 1**

Or [Prime members](#) get FREE delivery

Table of Contents

Welcome & Introduction.....	2
Gaia 4.18 Immersion: Tips, Tricks, and Best Practices Training Details.....	7
Module 1 – Gaia Origins & Prior Operating Systems.....	9
R82/Gaia 4.18 Updates: Summary.....	11
Tips, Tricks, & Best Practices.....	13
Data Sharing and AutoUpdater Silent Updates – Tips, Tricks, and Best Practices.....	13
Module 2 – Gaia on SMS/MDS vs. Security Gateways.....	16
R82/Gaia 4.18 Updates.....	17
Tips, Tricks, & Best Practices.....	17
Module 3 – Gaia on Check Point Appliances vs. Open Hardware vs. Cloud.....	18
R82/Gaia 4.18 Updates.....	19
Tips, Tricks, & Best Practices.....	19
Module 4 – The “Thin Pink Line” of Check Point & CPU Analysis.....	20
Gaia Kernel Versions – SMS/MDS/Log Server/SmartEvent Server.....	22
Gaia Kernel Versions – Security Gateways.....	23
User Space Firewall (USFW).....	24
Gaia Security Gateway CPU Usage Analysis.....	28
Top Output: “us” & “ni” – Process/User Space.....	29
Top Output: “sy” & “si” – System Space.....	30
Top Output: “wa” – Waiting for I/O Operation.....	30
Top Output: “hi” & “st” – HW Interrupts & “Stolen” CPU Cycles.....	32
Gaia SMS/MDS CPU Usage Analysis.....	33
Gaia Memory Usage Analysis.....	34
R82/Gaia 4.18 Updates.....	36
Tips, Tricks, & Best Practices.....	39
strace and the Undocumented "perf" Command: Tips, Tricks, and Best Practices.....	42
Using perf to Troubleshoot Persistent, Excessive CPU Utilization on a Particular Core.....	46
Module 5 – Interacting with Gaia Part 1: The CLI.....	50
Method 1 – The clish Shell.....	50
Maestro gclish.....	51
Method 2 – Expert Mode.....	54

R82/Gaia 4.18 Updates.....	57
Tips, Tricks, & Best Practices.....	61
The clish Shell – Tips, Tricks, & Best Practices.....	61
Maestro & the gclish Shell – Tips, Tricks, & Best Practices.....	62
"Global" Commands Outside a Scalable Platform/Maestro Environment – Tips, Tricks, & Best Practices.....	64
Module 6 – Interacting with Gaia Part 2: The Web Interface, Locks, & Gaia API.....	65
Method 1 – Gaia Web Interface.....	65
Gaia Authorized GUI Clients (SMS/MDS Only).....	68
CPUSE.....	69
Gaia Configuration Lock Mechanism.....	72
Method 2 – Gaia API.....	74
Method 3 – Central Deployment Tool (CDT).....	75
R82/Gaia 4.18 Updates.....	77
Tips, Tricks, & Best Practices.....	77
Module 7 – Interacting with Gaia Part 3: The SmartConsole GUI.....	79
CDT SmartConsole Integration.....	79
SmartConsole Command/Scripting Options.....	82
R82/Gaia 4.18 Updates.....	85
Tips, Tricks, & Best Practices.....	85
Module 8 – Gaia Network Interfaces, Bonding, & VLAN Tagging.....	86
Gaia Physical Interface Configuration.....	86
The Gaia Management Interface.....	89
Gaia VLAN (802.1q Tagged) Interface Configuration.....	91
Gaia Bonded Interface Configuration.....	96
Gaia Bridged Interface Configuration.....	103
Gaia Monitor/Tap Interface Configuration.....	106
R82/Gaia 4.18 Updates.....	108
Tips, Tricks, & Best Practices.....	110
Interface Tips, Tricks & Best Practices.....	110
Gateway General Bond Tips, Tricks & Best Practices.....	114
Maestro-specific Bond Tips, Tricks & Best Practices.....	116
Address Resolution Protocol (ARP) - Tips, Tricks & Best Practices.....	117

Module 9 – Gaia Routing.....	118
Gaia Static Route Configuration.....	118
Gaia Static Default Route Configuration.....	122
Gaia Dynamic Route Configuration.....	125
Gaia Policy-Based Routing.....	128
Gaia DHCP Relay.....	131
R82/Gaia 4.18 Updates.....	133
Tips, Tricks, & Best Practices.....	136
Gateway Static Routing Tips, Tricks, & Best Practices.....	136
Gateway Dynamic Routing – Tips, Tricks, & Best Practices.....	139
Network Testing Commands Tips, Tricks & Best Practices – traceroute/tracert/pathping/mtr.....	141
Module 10 – Gaia & ClusterXL/VRRP Clustering.....	148
Enable Clustering & cpconfig.....	148
Caution – Virtual Router Redundancy Protocol (VRRP).....	149
Accessing the Standby Member with SSH/HTTPS.....	151
R82/Gaia 4.18 Updates.....	153
Tips, Tricks, & Best Practices.....	155
Module 11 – Gaia Syslog Logging.....	159
Gaia Logging via Syslog.....	159
R82/Gaia 4.18 Updates.....	162
Tips, Tricks, & Best Practices.....	164
Module 12 – Gaia Backup Options.....	166
Method 1 – backup / restore.....	167
Method 2 – snapshot / revert (and R82 lightshots).....	174
Method 3 – Gaia save configuration / load configuration.....	177
R82/Gaia 4.18 Updates.....	178
Tips, Tricks, & Best Practices.....	180
Module 13 – Gaia OS Authentication Options.....	182
Gaia Administrative Accounts & SCP.....	185
External Gaia Authentication with RADIUS and TACACS+.....	186
R82/Gaia 4.18 Updates.....	191
Tips, Tricks, & Best Practices.....	198

Local Gaia Authentication Tips, Tricks & Best Practices.....	198
Ensuring Local Gaia Access Tips, Tricks, Best Practices.....	200
Recovering Access to Gaia Tips, Tricks, Best Practices.....	200
Gaia Remote Authentication Tips, Tricks & Best Practices.....	201
Gaia Two-Factor Authentication: Tips, Tricks, & Best Practices.....	203
Module 14 – Gaia Monitoring & Health.....	205
System Resource Monitoring.....	205
Hardware Health.....	210
SNMP Monitoring & Traps.....	215
NetFlow Monitoring.....	218
R82/Gaia 4.18 Updates.....	221
Tips, Tricks, & Best Practices.....	222
cpview/sar Tips, Tricks, & Best Practices.....	222
Hardware Monitoring Tips, Tricks, & Best Practices.....	226
SNMP/Netflow Tips, Tricks, & Best Practices.....	227
HealthCheck Point™ (HCP) Tips, Tricks, and Best Practices.....	227
HealthCheck Point™ (HCP) "Secret" TAC Tests – Tips, Tricks, & Best Practices.....	228
Module 15 – Gaia Packet Captures with tcpdump: The Basics.....	230
Workflow for tcpdump.....	230
Examples of tcpdump Filtering Syntax.....	233
R82/Gaia 4.18 Updates.....	234
Tips, Tricks, & Best Practices.....	235
Appendix A – R82.10 and Gaia Kernel 5.14.0-427.13.1 Preview.....	237
Wrap-up Discussion and Additional Resources.....	239

Gaia 4.18 Immersion: Tips, Tricks, and Best Practices Training Details

- *At the end of each module, there will be an **R82/Gaia 4.18 Updates** and a **Tips, Tricks, and Best Practices** section – these are always worth a quick look even if you are already intimately familiar with the topics covered by that module!*
- Prerequisites: Basic systems and networking knowledge. CCSA certification or equivalent experience helpful.
- This course is not intended to completely replace the extensive Check Point R82 formal documentation, which fully describes the Gaia OS and how to perform detailed, specific configurations. The intent is to provide overall guidance with some basic sample configurations, along with details of the new tools & features in Gaia 4.18, as well as providing the latest real-world tips, tricks, and best practices that are not always included in the formal documentation (or not even documented at all).
- The slides we will be working with in the recorded videos are identical to those provided in this PDF document.
- We will be working with the Gaia OS version associated with the R82 GA release (Red Hat Enterprise Linux [RHEL] 8.6 with kernel 4.18). We will also mention the older 3.10 kernel used in R81.20 and earlier code releases, dating back to version R80.40.
- It is anticipated that version R82.10, currently in private Early Availability (EA) as of this writing, will update the Linux kernel to 5.14.0-427.13.1 (the equivalent of RHEL 9.4). This update is primarily to obtain support for the ARM CPUs in use on the new 3900 series appliances: [sk183199: Quantum Force 3900 Appliances](#). The Gaia-level changes of this update to kernel 5.14.0-427.13.1 are anticipated to be minor and are previewed in Appendix A.
- The course assumes working with a Gaia system that has already been imaged and deployed (or upgraded) with R82. The Gaia imaging process, via tools such as [ISOMorphic](#) and [Blink](#), is well-documented by Check Point and not covered in this course. If the Gaia imaging and deployment tasks are of interest, I'd strongly recommend checking out the upcoming [Check Point Deployment Administrator \(CPDA\)](#) R82 course, which should be available from Check Point ATC partners worldwide soon. Blink is covered (and utilized) in the existing [Check Point Automation Specialist \(CCAS\)](#) R81.20 course which is already available from ATCs worldwide including Shadow Peak. The official [R82 Upgrade & Installation Guide](#) always contains the latest R82 upgrade information & procedures.

- The primary focus of this course is the Gaia 4.18 kernel running on Check Point appliances (models 3000-29XXX), including gateway appliances being utilized for Maestro Security Groups. Maestro Hyperscale Orchestrators will have limited coverage, as will the Scalable Platform chassis.
- The material presented in this course will mostly apply to CloudGuard gateways (which also utilize the same RHEL 8.6 Gaia 4.18 OS), subject to the documented R82 CloudGuard Controller Administration Guide [Limitations](#).
- Embedded Gaia, based on the Linux BusyBox OS and used on the 600-2000 appliance models called "Quantum Spark", will have limited coverage in this course; however, the concepts and most configuration operations are similar. Differences between Embedded Gaia and "maintrain" Gaia are documented here: [sk178604: Check Point R81.10.X for 1500, 1600, 1800, 1900, and 2000 appliance Known Limitations](#)
- Hyperlinks shown in this document are “hot” and can be clicked to show the specified resource in your web browser. Hyperlinked references are provided in this course for two reasons: further reading if the subject is of particular interest to you, and also to provide the very latest information about the topic after the publication of this course.