



---

# TRUSTED, ACCURATE AND RELIABLE!

---

The most comprehensive IT certification  
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

<https://www.virtulearner.com>  
[support@virtulearner.com](mailto:support@virtulearner.com)

**CheckPoint**

**156-587**

Check Point Certified  
Troubleshooting Expert -  
R81.20

**QUESTION: 1**

You run a free-command on a gateway and notice that the Swap column is not zero Choose the best answer

- A. Utilization of ram is high and swap file had to be used
- B. Swap file is used regularly because RAM memory is reserved for management traffic
- C. Swap memory is used for heavy connections when RAM memory is full
- D. Its ole Swap is used to increase performance

**Answer(s):** A

**QUESTION: 2**

You modified kernel parameters and after rebooting the gateway, a lot of production traffic gets dropped and the gateway acts strangely What should you do"?

- A. Run command fw ctl set int fw1\_kernel\_all\_disable=1
- B. Restore fwkem.conf from backup and reboot the gateway
- C. run fw unloadlocal to remove parameters from kernel
- D. Remove all kernel parameters from fwkem.conf and reboot

**Answer(s):** B

**Explanation:**

If you have modified kernel parameters (in fwkern.conf, for example) and the gateway starts dropping traffic or behaving abnormally after a reboot, the best practice is to restore the original or a known-good configuration from backup. Then, reboot again so that the gateway loads the last known stable settings.

Option A (fw ctl set int fw1\_kernel\_all\_disable=1) is not a standard or documented method for "undoing" all kernel tweaks.

Option B (Restore fwkem.conf from backup and reboot the gateway) is the correct and straightforward approach.

Option C (fw unloadlocal) removes the local policy but does not revert custom kernel parameters that have already been loaded at boot.

Option D (Remove all kernel parameters from fwkem.conf and reboot) might help in some cases, but you risk losing other beneficial or necessary parameters if there were legitimate custom settings. Restoring from a known-good backup is safer and more precise.

Hence, the best answer:

"Restore fwkem.conf from backup and reboot the gateway."

Check Point Troubleshooting Reference sk98339 - Working with fwkern.conf (kernel parameters) in Gaia OS.

sk92739 - Advanced System Tuning in Gaia OS.

Check Point Gaia Administration Guide - Section on kernel parameters and system tuning.

Check Point CLI Reference Guide - Explanation of using fw ctl, fw unloadlocal, and relevant troubleshooting commands.

**QUESTION: 3**

What process monitors terminates, and restarts critical Check Point processes as necessary?

- A. CPM
- B. FWD
- C. CPWD
- D. FWM

**Answer(s): C**

**Explanation:**

CPWD (Check Point WatchDog) is the process that monitors, terminates (if necessary), and restarts critical Check Point processes (e.g., FWD, FWM, CPM) when they stop responding or crash.

CPM (Check Point Management process) is a process on the Management Server responsible for the web-based SmartConsole connections, policy installations, etc.

FWD (Firewall Daemon) handles logging and communication functions in the Security Gateway.

FWM (FireWall Management) is an older reference to the management process on the Management Server for older versions.

Therefore, the best answer is CPWD.

Check Point Troubleshooting Reference sk97638: Check Point WatchDog (CPWD) process explanation and commands.

R81.20 Administration Guide - Section on CoreXL, Daemons, and CPWD usage.

sk105217: Best Practices - Explains system processes, how to monitor them, and how CPWD is utilized.

**QUESTION: 4**

When dealing with monolithic operating systems such as Gaia where are system calls initiated from to achieve a required system level function?

- A. Kernel Mode
- B. Slow Path
- C. Medium Path
- D. User Mode

**Answer(s): A**