



# 156-585<sup>Q&As</sup>

Check Point Certified Troubleshooting Expert

## Pass CheckPoint 156-585 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/156-585.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

What is the simplest and most efficient way to check all dropped packets in real time?

- A. fw ctl zdebug \* drop in expert mode
- B. Smartlog
- C. cat /dev/fwTlog in expert mode
- D. tail -f SFWDIR/log/fw log |grep drop in expert mode

Correct Answer: D

---

**QUESTION 2**

When a User Mode process suddenly crashes it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash? i Program Counter ii Stack Pointer

ii.

Memory management information iv Other Processor and OS flags / information

A.

i, ii, lii and iv

B.

i and n only

C.

iii and iv only

D.

Only iii

Correct Answer: C

---

**QUESTION 3**

The Check Point Firewall Kernel is the core component of the Gala operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

- A. fw ctl debug/kdebug



- B. fw ctl zdebug
- C. fw debug/kdebug
- D. fw debug/kdebug ctl

Correct Answer: A

fw ctl zdebug is only for drops and fw ctl debug/kdebug are more detailed and flexible

---

#### QUESTION 4

What acceleration mode utilizes multi-core processing to assist with traffic processing?

- A. CoreXL
- B. SecureXL
- C. HyperThreading
- D. Traffic Warping

Correct Answer: C

---

#### QUESTION 5

What is the main SecureXL database for tracking acceleration status of traffic?

- A. cphwd\_db
- B. cphwd\_tmp1
- C. cphwd\_dev\_conn\_table
- D. cphwd\_dev\_identity\_table

Correct Answer: B

[156-585 PDF Dumps](#)

[156-585 VCE Dumps](#)

[156-585 Brindumps](#)