

## 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.leads4pass.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

The Check Point Firewall Kernel is the core component of the Galia 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 2

Troubleshooting issues with Mobile Access requires the following:

- A. Standard VPN debugs, packet captures, and debugs of cvpnd process on Security Gateway
- B. Standard VPN debugs and packet captures on Security Gateway, debugs of "cvpnd" process on Security Management
- C. "ma\_vpn" process on Security Gateway
- D. Debug logs of FWD captured with the command - "fw debug fwd on TDERROR\_MOBILE\_ACCESS=5"

Correct Answer: A

---

## QUESTION 3

Select the technology that does the following actions

- provides reassembly via streaming for TCP
  - handles packet reordering and congestion
  - handles payload overlap
  - provides consistent stream of data to protocol parsers
- A. Passive Streaming Library
  - B. Context Management
  - C. Pre-Protocol Parser

D. fwtcpstream

Correct Answer: A

---

## QUESTION 4

Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, choose the correct answer.

A. fw monitor -po -0x1ffffe0

B. fw monitor -p0 0x1ffffe0

C. fw monitor -po 1ffffe0

D. fw monitor -p0 -0x1ffffe0

Correct Answer: A

[https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP\\_R80.40\\_PerformanceTuning\\_AdminGuide/Content/Topics-PTG/CLI/fw-monitor.htm](https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/CLI/fw-monitor.htm)

---

## QUESTION 5

If the cpsemd process of SmartEvent has crashed or is having trouble coming up, then it usually indicates that\_\_\_\_\_.

A. Postgres database is down

B. Cpd daemon is unable to connect to the log server

C. The SmartEvent core on the Solr indexer has been deleted

D. The logged in administrator does not have permissions to run SmartEvent

Correct Answer: A

cpsemd is the process responsible for logging into the SmartEvent GUI. Therefore, you need to check the status of this process and debug it, if necessary. Usually, the issue with the cpsemd process is that it is crashing, or not coming up. What causes this process to crash or not come up is that the PostgreSQL database is down. Therefore, in order to run the cpsemd process successfully, you need to run the PostgreSQL database successfully.

[Latest 156-585 Dumps](#)

[156-585 VCE Dumps](#)

[156-585 Exam Questions](#)