# 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**

What is the benefit of running "vpn debug trunc over "vpn debug on"?

A. "vpn debug trunc" purges ike.elg and vpnd elg and creates limestarnp while starting ike debug and vpn debug

B. "vpn debug trunc* truncates the capture hence the output contains minimal capture

C. "vpn debug trunc* provides verbose capture

D. No advantage one over the other

Correct Answer: A

**QUESTION 2**

Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump

B. CPMIL dump

C. fw monitor

D. tcpdump

Correct Answer: A

**QUESTION 3**

For TCP connections, when a packet arrives at the Firewall Kemel out of sequence or fragmented, which layer of IPS corrects this lo allow for proper inspection?

A. Passive Streaming Library

B. Protections

C. Protocol Parsers

D. Context Management

Correct Answer: D

**QUESTION 4**

What is the most efficient way to view large fw monitor captures and run filters on the file?

A. wireshark

B. CLISH

C. CLI

D. snoop

Correct Answer: A

---

**QUESTION 5**

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

---