



156-585^{Q&As}

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.passapply.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

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

- A. Passive Streaming Library
- B. Protections
- C. Protocol Parsers
- D. Context Management

Correct Answer: D

QUESTION 2

When debugging is enabled on firewall kernel module using the ``fw ctl debug\`` command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?

- A. Messages are written to a buffer and collected using ``fw ctl kdebug\``
- B. Messages are written to console and also `/var/log/messages` file
- C. Messages are written to `/etc/dmesg` file
- D. Messages are written to `$FWDIR/log/fw.elg`

Correct Answer: B

QUESTION 3

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

QUESTION 4

What are the main components of Check Point's Security Management architecture?



- A. Management server, management database, log server, automation server
- B. Management server, Security Gateway. Multi-Domain Server, SmartEvent Server
- C. Management Server. Log Server. LDAP Server, Web Server
- D. Management server Log server, Gateway server. Security server

Correct Answer: A

QUESTION 5

What command sets a specific interface as not accelerated?

- A. noaccel-s
- B. fwaccel exempt state
- C. nonaccel -s
- D. fwaccel -n

Correct Answer: C

[Latest 156-585 Dumps](#)

[156-585 Practice Test](#)

[156-585 Study Guide](#)