



# 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.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

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 2

Which command is most useful for debugging the fwaccel module?

- A. fw zdebug
- B. securexl debug
- C. fwaccel dbg
- D. fw debug

Correct Answer: C

---

#### QUESTION 3

What is the proper command for allowing the system to create core files?

- A. \$FWDIR/scripts/core-dump-enable.sh
- B. # set core-dump enable # save config
- C. service core-dump start
- D. >set core-dump enable >save config

Correct Answer: D

---

#### QUESTION 4

What table does command "fwaccel conns" pull information from?

- A. fwxl\_conns
- B. SecureXLCon



C. cphwd\_db

D. sxl\_connections

Correct Answer: A

---

#### QUESTION 5

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

[Latest 156-585 Dumps](#)

[156-585 PDF Dumps](#)

[156-585 Study Guide](#)