



# 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.geekcert.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

John has renewed his NGTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CU of the gateway, what command can he use for this?

- A. cpstat antimalware -f subscription\_status
- B. fw monitor license status
- C. fwm lie print
- D. show license status

Correct Answer: A

---

### QUESTION 2

Which of the following inputs is suitable for debugging HTTPS inspection issues?

- A. vpn debug cpts on
- B. fw ctl debug ? fw + conn drop cpts
- C. fw diag debug tls enable
- D. fw debug tls on TDERROR\_ALL\_ALL=5

Correct Answer: B

Reference: [https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&andsolutioid=sk108202](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&andsolutioid=sk108202)

---

### QUESTION 3

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

- A. fwxl\_conns
- B. SecureXLCon
- C. cphwd\_db
- D. sxl\_connections

Correct Answer: A

---

### QUESTION 4

How can you start debug of the Unified Policy with all possible flags turned on?



- A. fw ctl debug -m UP all
- B. fw ctl debug -m UnifiedPolicy all
- C. fw ctl debug -m fw + UP
- D. fw ctl debug -m UP \*

Correct Answer: D

#### QUESTION 5

The two procedures available for debugging in the firewall kernel are i fw ctl zdebug ii fw ctl debug/kdebug Choose the correct statement explaining the differences in the two

- A. (i) Is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command line whereas  
(ii) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line
- B. (i) is used to debug the access control policy only, however  
(ii) can be used to debug a unified policy
- C. (i) is used to debug only issues related to dropping of traffic, however  
(ii) can be used for any firewall issue including NATing, clustering etc.
- D. (i) is used on a Security Gateway, whereas  
(ii) is used on a Security Management Server

Correct Answer: A

According to the study material, this should be A:

The Zdebug has a 1 MB buffer, cleans the buffer, enable flags and collects debug messages from the kernel for you.

According to C, it is used for drop traffic, this is completely false

You can set modules on it as well, such as CCP, cluster, fw, drop etc.

Debug requires more configuration to be effective, but gives you more opportunities to play with, therefore, A is the correct answer.