

TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!



Exam : **156-115.77**

Title : Check Point Certified
Security Master

Version : DEMO

1.What command would you use for a packet capture on an absolute position for TCP streaming (out) 1ffffe0

- A. fw ctl chain -po 1ffffe0 -o monitor.out
- B. fw monitor -po -0x1ffffe0 -o monitor.out
- C. fw monitor -e 0x1ffffe0 -o monitor.out
- D. fw monitor -pr 1ffffe0 -o monitor.out

Answer: B

2.The command fw monitor -p all displays what type of information?

- A. It captures all points of the chain as the packet goes through the firewall kernel.
- B. This is not a valid command.
- C. The -p is used to resolve MAC address in the firewall capture.
- D. It does a firewall monitor capture on all interfaces.

Answer: A

3.What does the IP Options Strip represent under the fw chain output?

- A. IP Options Strip is not a valid fw chain output.
- B. The IP Options Strip removes the IP header of the packet prior to be passed to the other kernel functions.
- C. The IP Options Strip copies the header details to forward the details for further IPS inspections.
- D. IP Options Strip is only used when VPN is involved.

Answer: B

4.The command that lists the firewall kernel modules on a Security Gateway is:

- A. fw list kernel modules
- B. fw ctl kernel chain
- C. fw ctl debug -m
- D. fw list modules

Answer: C

5.Which of the following BEST describes the command fw ctl chain function?

- A. View how CoreXL is distributing traffic among the firewall kernel instances.
- B. View established connections in the connections table.
- C. View the inbound and outbound kernel modules and the order in which they are applied.
- D. Determine if VPN Security Associations are being established.

Answer: C