**Vendor:**CheckPoint

**Exam Code:**156-115.80

**Exam Name:**Check Point Certified Security Master - R80

**Version:**Demo

**QUESTION 1**

Fill in the blank: The R80 utility fw monitor is used to troubleshoot _____.

A. User data base corruption

B. LDAP conflicts

C. Traffic issues

D. Phase two key negotiation

Correct Answer: C

---

**QUESTION 2**

Which of the following is NOT a special consideration while running fw monitor on production firewall?

A. While executing fw monitor, you need to specify an expression so that it captures the required traffic instead of all traffic

B. While running fw monitor on a busy firewall, the –ci and –co switches can be used to limit the number of packets captured

C. While running fw monitor, it resets all the debug flags

D. During a fw monitor, the firewall will have to process more packets because SecureXL acceleration should be disabled

Correct Answer: C

---

**QUESTION 3**

The fw monitor output file type is?

A. Binary

B. ASCII text

C. ZIP

D. tar.gzip

Correct Answer: B

---

**QUESTION 4**

Which command would you use to check CoreXL instances for IPv6 traffic?

A. fwaccel6 stats

B. fwaccel6 stat

C. fw ctl multik stat

D. fw6ctl multik stat

Correct Answer: C

---

**QUESTION 5**

Having a look at the output of the "fwaccel conns" command, the F flag is the indicator for a packet _____.

A. getting the routing information according to the Forwarding Information Base (FIB)

B. being processed by the firewall kernel module

C. going through the slow path

D. being forced of using the accelerated path

Correct Answer: B

---

**QUESTION 6**

Consider the IPv6 address: 2101:0DA0:080B:4114:0000:0000:0000:0001. According to IPv6 IP shortening rules, what address can this be shortened to?

A. 2101:0DA0:080B:4114::8:0

B. 2101:0DA0:80B:4114::0

C. 2101:0DA0:080B:4114::8:1

D. 2101:0DA0:80B:4114::1

Correct Answer: D

---

**QUESTION 7**

By default, how long does the UDP connection remain on the state table?

A. 30 Seconds

B. 30 minutes

C. 60 minutes

D. 40 Seconds

Correct Answer: D

Reference: https://community.checkpoint.com/t5/General-Topics/R80-x-Performance-Tuning-TipConnection-Table/td-p/41581#:~:text=For%20example%2C%20the%20default%20session,(TCP%20to% 203600%20seconds).

---

**QUESTION 8**

Which of the following would NOT be a flag when debugging a unified policy?

A. rulebase

B. clob

C. connection

D. tls

Correct Answer: D

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk120964

---

**QUESTION 9**

When troubleshooting static NAT, you would follow all the steps below, EXCEPT:

A. Verify NAT configuration

B. Debug NAT

C. Run "fw tab -t fwx_alloc"

D. Run "fw ctl arp" command

Correct Answer: C

---

**QUESTION 10**

Which of the following is NOT a valid "fwaccel" parameter?

A. stat

B. stats

C. templates

D. packets

Correct Answer: D

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk41397

---

**QUESTION 11**

You suspect that IPS protections may be dropping legitimate traffic by mistake. To reduce the false positives, what GuiDBedit parameter could you enable to work with fw ctl zdebug drop to generate a more elaborate drop message for these packets?

A. enable_inspect_debug_ips_compilation

B. inspect_ips_debug_inspection

C. enable_inspect_debug_compilation

D. enable_inspect_debug_ips

Correct Answer: C

---

**QUESTION 12**

Consider a Check Point Security Gateway under high load. What mechanism can be used to confirm that important traffic such as control connections are not dropped?

A. fw debug fgd50 on OPSEC_DEBUG_LEVEL=3

B. fw ctl multik prioq

C. fgate –d load

D. fw ctl debug –m fg all

Correct Answer: B