NSE7_EFW-6.0$^{Q\&As}$

Fortinet NSE 7 - Enterprise Firewall 6.0

Pass Fortinet NSE7_EFW-6.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse7_efw-6-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any \\'esp\\'

B. diagnose sniffer packet any \\'tcp port 500 or tcp port 4500\\'

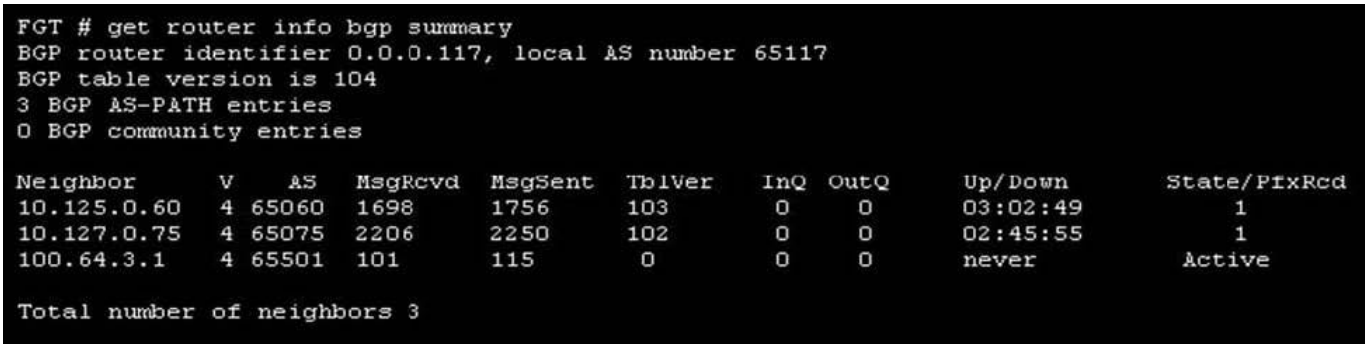
C. diagnose sniffer packet any \\'udp port 4500\\'

D. diagnose sniffer packet any \\'udp port 500\\'

Correct Answer: A

QUESTION 2

View the exhibit, which contains the output of a BGP debug command, and then answer the question below.



```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V    AS   MsgRcvd  MsgSent  TblVer   InQ  OutQ    Up/Down       State/PfxRcd
10.125.0.60   4  65060  1698     1756     103        0     0    03:02:49             1
10.127.0.75   4  65075  2206     2250     102        0     0    02:45:55             1
100.64.3.1    4  65501  101      115        0        0     0    never             Active

Total number of neighbors 3
```

Which of the following statements about the exhibit are true? (Choose two.)

A. The local router\\'s BGP state is Established with the 10.125.0.60 peer.

B. Since the counters were last reset; the 10.200.3.1 peer has never been down.

C. The local router has received a total of three BGP prefixes from all peers.

D. The local router has not established a TCP session with 100.64.3.1.

Correct Answer: AD

QUESTION 3

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filler web requests when the client browser does not provide the server name indication (SNI) extension ?

A. FortiGate switches to the full SSL inspection method to decrypt the data.

B. FortiGate blocks the request without any further inspection.

C. FortiGate uses the Issued T: field in the server\\'s certificate.

D. FortiGate uses the requested URL from the user\\'s web browser.

Correct Answer: C

QUESTION 4

What configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. mem-failopen

B. ips-failopen

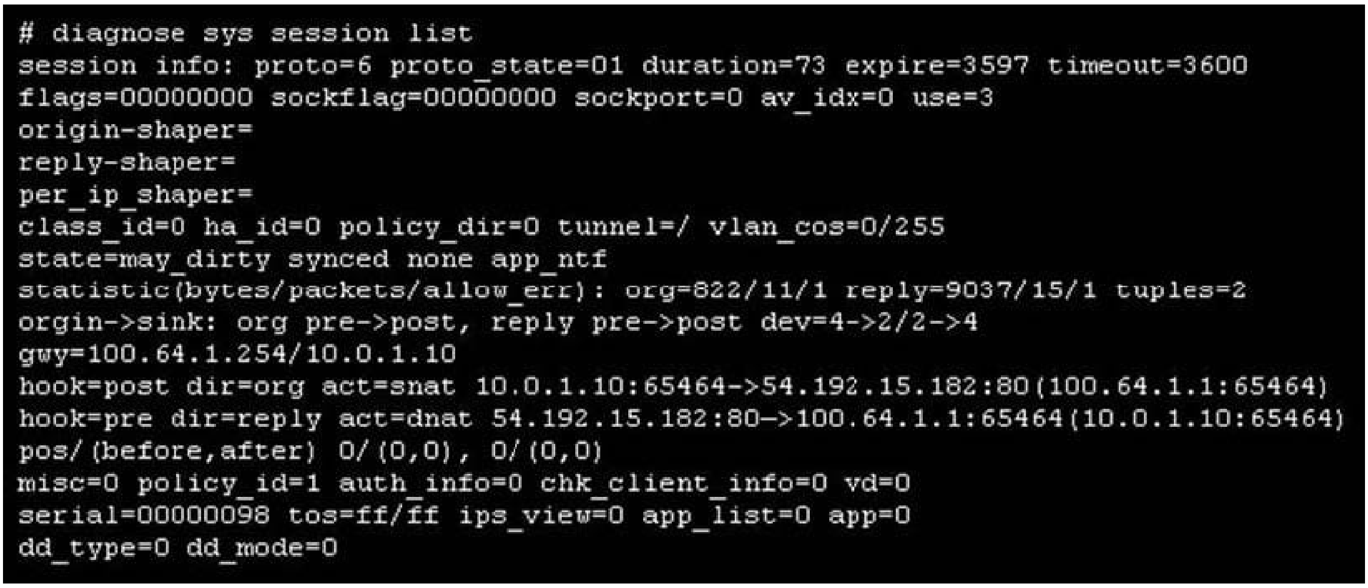
C. utm-failopen

D. av-failopen

Correct Answer: BD

QUESTION 5

View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.



```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which one of the following statements about the output is true?

A. This session is for HA heartbeat traffic.

B. This session cannot be synced with the slave unit.

C. The master unit is processing this traffic.

D. The inspection of this session has been offloaded to the slave unit.

Correct Answer: C