Free Questions for FCSS_NST_SE-7.4

Shared by Campos on 11-10-2024

Question 1

Question Type: MultipleChoice

Which two statements about conserve mode are true? (Choose two.)

Options:

A- FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.

B- FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.

C- FortiGate exits conserve mode when the system memory goes below the configured green threshold.

D- FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.

Answer:

B, C

Question 2

Question Type: MultipleChoice

Which statement about protocol options is true?

Options:

A- Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.

B- Protocol options give administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.

C- Protocol options allow administrators to configure the Any setting for all enabled protocols, which provides the most efficient use of system resources.

D- Protocol options allow administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

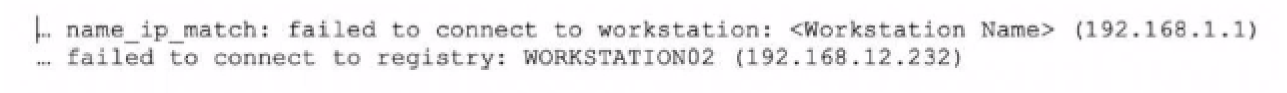
Answer:

D

Question 3

Question Type: **MultipleChoice**

Exhibit.



```
|… name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
 … failed to connect to registry: WORKSTATION02 (192.168.12.232)
```

Refer to the exhibit, which shows two entries that were generated in the FSSO collector agent logs.

What three conclusions can you draw from these log entries? {Choose three.)

Options:

A- Remote registry is not running on the workstation.

B- The user's status shows as 'not verified' in the collector agent.

C- DNS resolution is unable to resolve the workstation name.

D- The FortiGate firmware version is not compatible with that of the collector agent.

E- A firewall is blocking traffic to port 139 and 445.

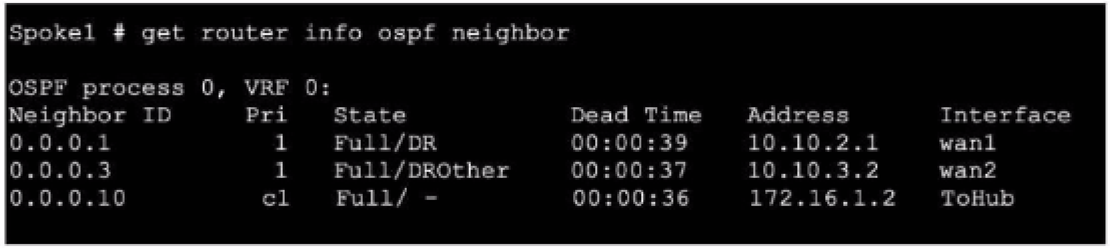
Answer:

A, B, E

Question 4

Question Type: MultipleChoice

Refer to the exhibit, which shows the output of get router info ospf neighbor.



```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address       Interface
0.0.0.1           1   Full/DR         00:00:39    10.10.2.1     wan1
0.0.0.3           1   Full/DROther    00:00:37    10.10.3.2     wan2
0.0.0.10         cl   Full/ -         00:00:36    172.16.1.2    ToHub
```

What can you conclude from the command output?

Options:

A- The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to-point.

B- All neighbors are in area 0.0.0.0.

C- The local FortiGate is the BDR.

D- The local FortiGate is not a DROther.

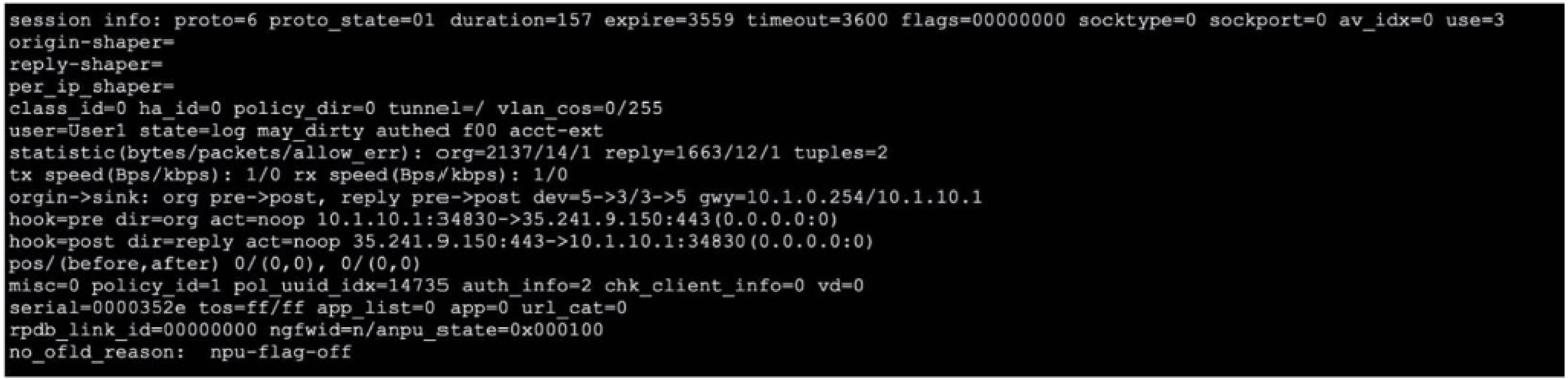
Answer:

A

Question 5

Question Type: MultipleChoice

Exhibit.



```
session info: proto=6 proto_state=01 duration=157 expire=3559 timeout=3600 flags=00000000 socktype=0 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
user=User1 state=log may_dirty authed f00 acct-ext
statistic(bytes/packets/allow_err): org=2137/14/1 reply=1663/12/1 tuples=2
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 1/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.0.254/10.1.10.1
hook=pre dir=org act=noop 10.1.10.1:34830->35.241.9.150:443(0.0.0.0:0)
hook=post dir=reply act=noop 35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/anpu_state=0x000100
no_ofld_reason:  npu-flag-off
```

Refer to the exhibit, which shows the output of a session. Which two statements are true? (Choose Iwo.)

Options:

A- The TCP session has been successfully established.

B- The session was initiated from an authenticated user.

C- The session is being inspected using flow inspection.

D- The session is being offloaded.

Answer:

A, B

Question 6

Question Type: **MultipleChoice**

What are two reasons you might see iprope_in_check() check failed, drop when using the debug flow? (Choose two.)

Options:

A- Packet was dropped because of policy route misconfiguration.

B- Packet was dropped because of traffic shaping.

C- Trusted host list misconfiguration.

D- VIP or IP pool misconfiguration.

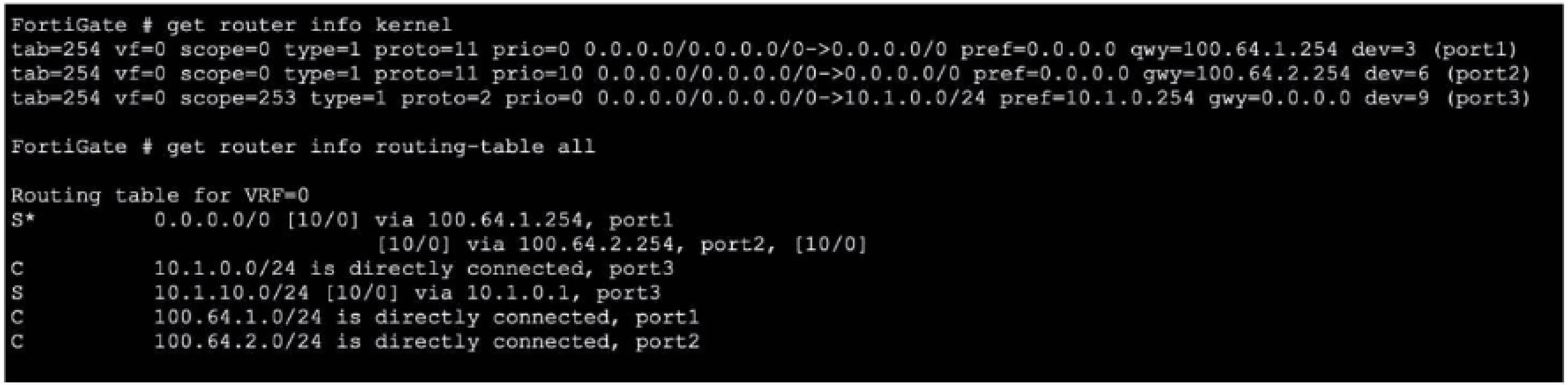
Answer:

C, D

Question 7

Question Type: MultipleChoice

Refer to the exhibit, which shows partial outputs from two routing debug commands.



```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 qwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*          0.0.0.0/0 [10/0] via 100.64.1.254, port1
                      [10/0] via 100.64.2.254, port2, [10/0]
C           10.1.0.0/24 is directly connected, port3
S           10.1.10.0/24 [10/0] via 10.1.0.1, port3
C           100.64.1.0/24 is directly connected, port1
C           100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

Options:

A- Set snat-route-change to enable.

B- Set the priority of the static default route using port2 to 1.

C- Set preserve-session-route to enable.

D- Set the priority of the static default route using port1 to 10.

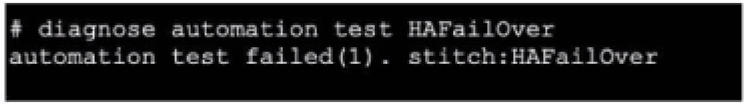
Answer:

D

Question 8

Question Type: MultipleChoice

Exhibit.



```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

Refer to the exhibit, which shows the output of diagnose automation test.

What can you observe from the output? (Choose two.)

Options:

A- The automation stitch test is not being logged.

B- The automation stitch test failed but the HA failover was successful.

C- An HA failover occurred.

D- The test was unsuccessful.

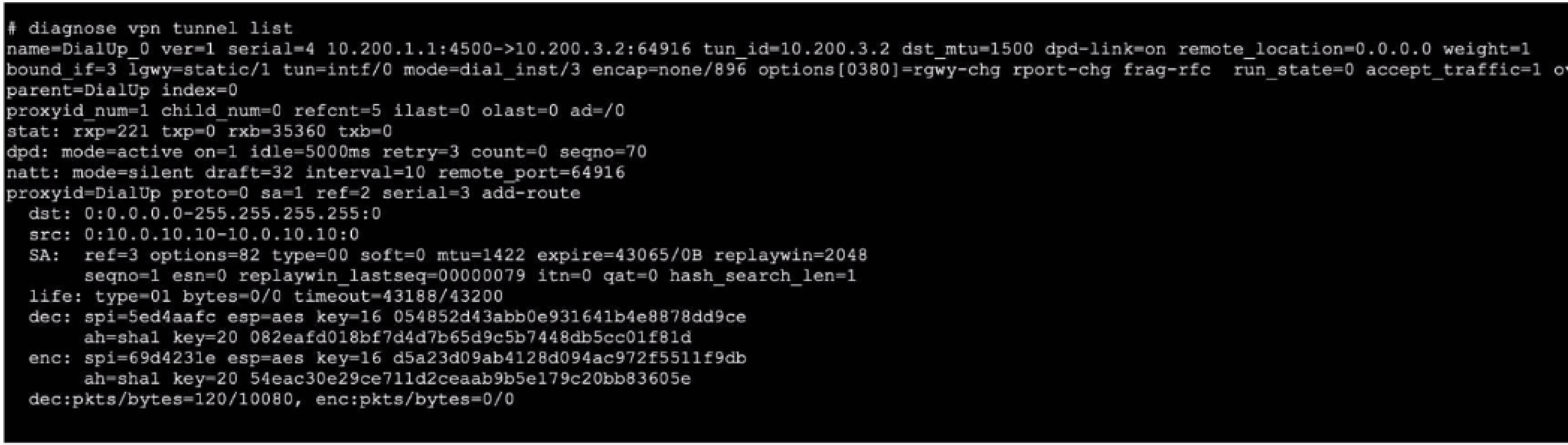
Answer:

A, D

Question 9

Question Type: MultipleChoice

Refer to the exhibit, which contains the output of diagnose vpn tunnel list.



```
# diagnose vpn tunnel list
name=DialUp_0 ver=1 serial=4 10.200.1.1:4500->10.200.3.2:64916 tun_id=10.200.3.2 dst_mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc  run_state=0 accept_traffic=1 o
parent=DialUp index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=221 txp=0 rxb=35360 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=70
natt: mode=silent draft=32 interval=10 remote_port=64916
proxyid=DialUp proto=0 sa=1 ref=2 serial=3 add-route
  dst: 0:0.0.0.0-255.255.255.255:0
  src: 0:10.0.10.10-10.0.10.10:0
  SA:  ref=3 options=82 type=00 soft=0 mtu=1422 expire=43065/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000079 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=5ed4aafc esp=aes key=16 054852d43abb0e931641b4e8878dd9ce
       ah=sha1 key=20 082eafd018bf7d4d7b65d9c5b7448db5cc01f81d
  enc: spi=69d4231e esp=aes key=16 d5a23d09ab4128d094ac972f5511f9db
       ah=sha1 key=20 54eac30e29ce711d2ceaab9b5e179c20bb83605e
  dec:pkts/bytes=120/10080, enc:pkts/bytes=0/0
```

Which command will capture ESP traffic for the VPN named DialUp_0?

Options:

A- diagnose sniffer packet any 'ip proto 50'

B- diagnose sniffer packet any 'host 10.0.10.10'

C- diagnose sniffer packet any 'esp and host 10.200.3.2'

D- diagnose sniffer packet any 'port 4500'

Answer:

D