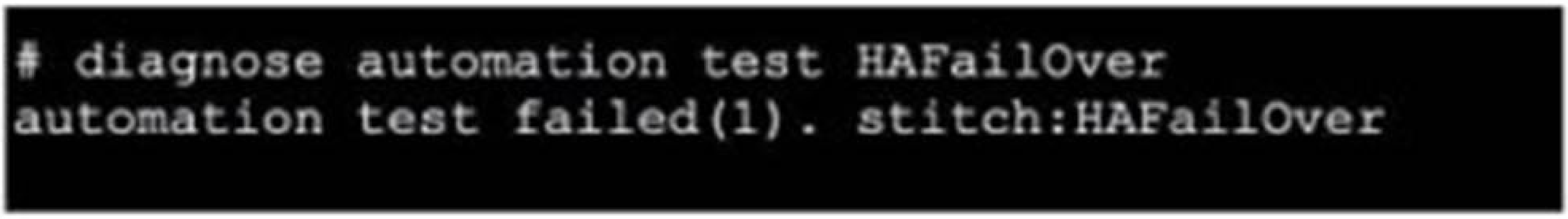
Exam Questions FCSS_NST_SE-7.4

FCSS - Network Security 7.4 Support Engineer

https://www.2passeasy.com/dumps/FCSS_NST_SE-7.4/

NEW QUESTION 1
Exhibit.



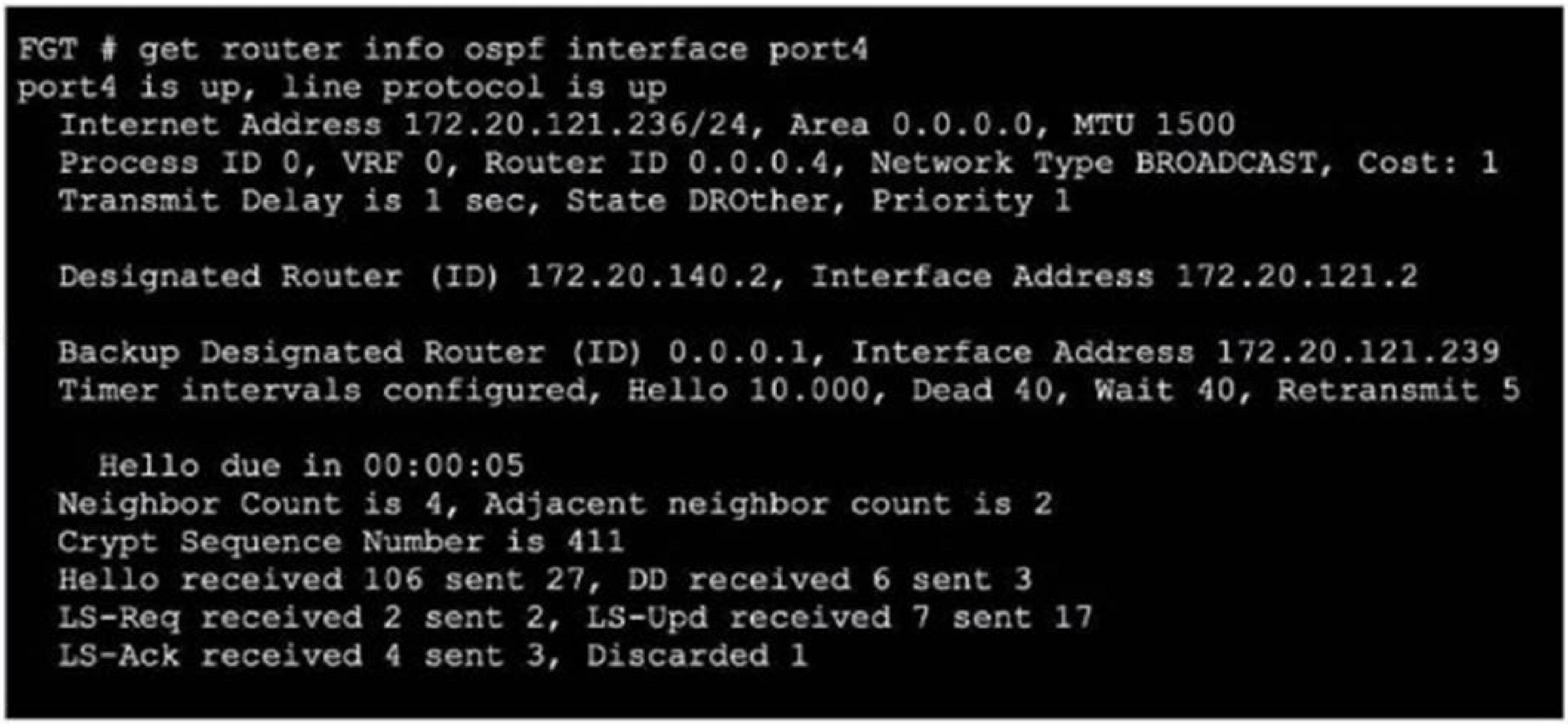
```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

Refer to the exhibit, which shows the output of diagnose automation test. What can you observe from the output? (Choose two.)

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: AD

NEW QUESTION 2
Refer to the exhibit, which shows the output ofa debug command.



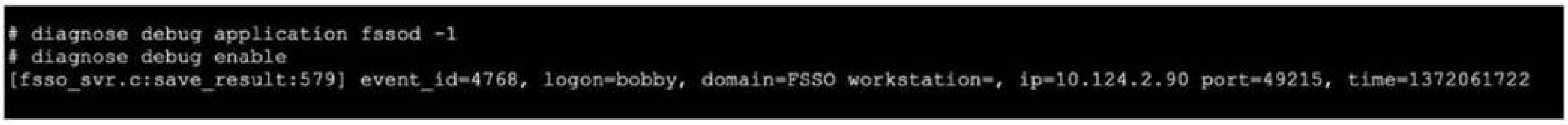
```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, VRF 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1

  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2

  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5

    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 sent 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

Which two statements about the output are true? (Choose two.)

A. The interlace is part of the OSPF backbone area.
B. There are a total of five OSPF routers attached to the vorz4 network segment
C. One of the neighbors has a router ID of 0.0.0.4.
D. In the network connected to port4, two OSPF routers are down.

Answer: AD

NEW QUESTION 3
Refer to the exhibit, which shows a partial output of the fssod daemon real-time debug command.



```
# diagnose debug application fssod -1
# diagnose debug enable
[fsso_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO workstation=, ip=10.124.2.90 port=49215, time=1372061722
```

What two conclusions can you draw Itom the output? (Choose two.)

A. The workstation with IP 10.124.2.90 will be polled frequently using TCP port 445 to see if the user is still logged on.
B. The logon event can be seen on the collector agent installed on Windows.
C. FSSO is using DC agent mode to detect logon events.
D. FSSO is using agentless polling mode to detect logon events.

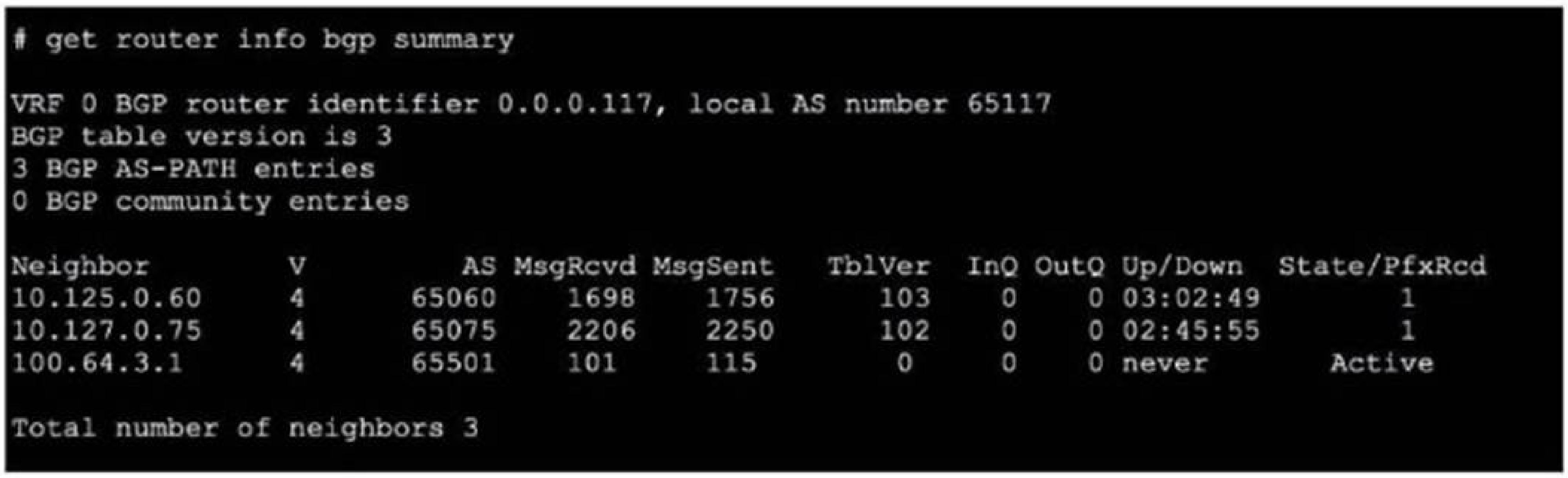
Answer: AD

NEW QUESTION 4
An administrator wants to capture encrypted phase 2 traffic between two FotiGate devices using the built-in sniffer.
If the administrator knows that there Is no NAT device located between both FortiGate devices, which command should the administrator run?

A. diagnose sniffer packet any 'udp port 500'
B. diagnose sniffer packet any 'lp proto 50'
C. diagnose sniffer packet any 'udp port 4500'
D. diagnose sniffer packet any 'ah'

Answer: B

NEW QUESTION 5
Refer to the exhibit, which shows the output of a BGP debug command.



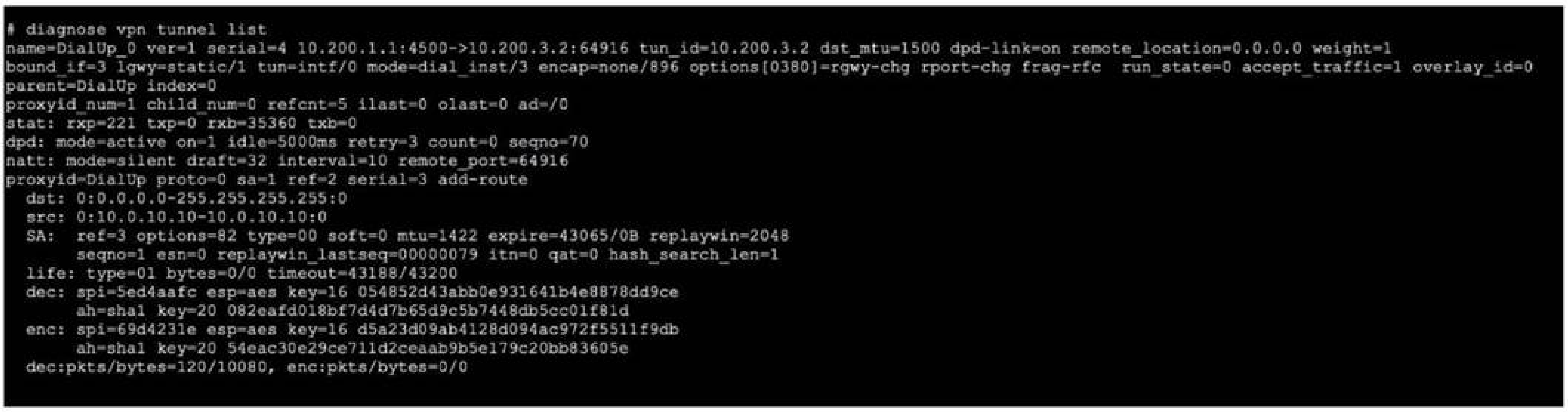
```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
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
```

Whatcan you conclude about the router in this scenario?

A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the 8GP session with the local router.
B. An inbound route-map on local router is blocking the prefixes from neighbor 100.64.3.1.
C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
D. The BGP session with peer 10.127.0.75 is up.

Answer: D

NEW QUESTION 6
Refer to the exhibit, which contains the output ofdiagnose vpn tunnellist.



```
# 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 overlay_id=0
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?

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'

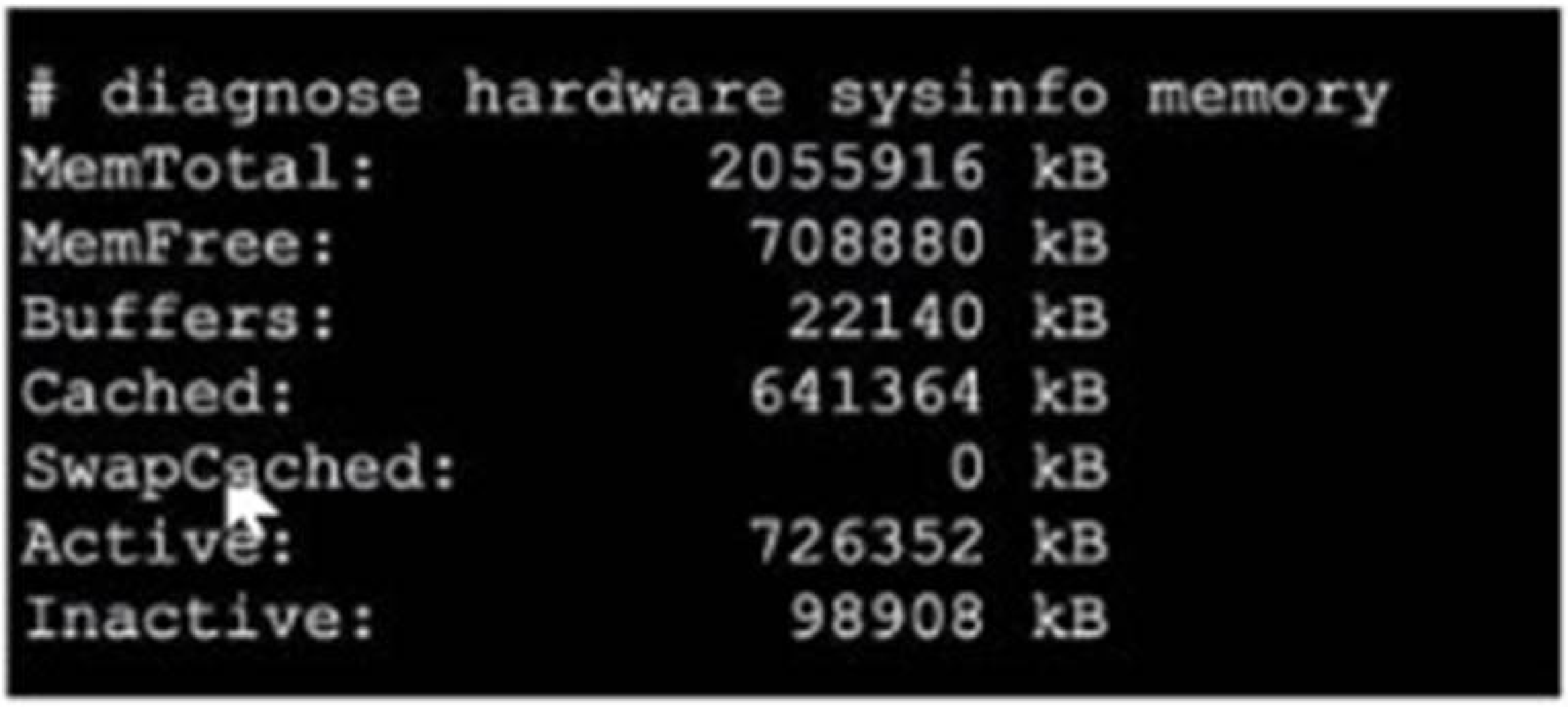
Answer: D

NEW QUESTION 7
Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.
Which action will FortiGate take when using the default settings for SSL certificate inspection?

A. FortiGate uses the SNI from the user's web browser.
B. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
C. FortiGate uses the first entry listed in the SAN field in the server certificate.
D. FortiGate uses the ZN information from the Subject field in the server certificate.

Answer: C

NEW QUESTION 8
Exhibit.



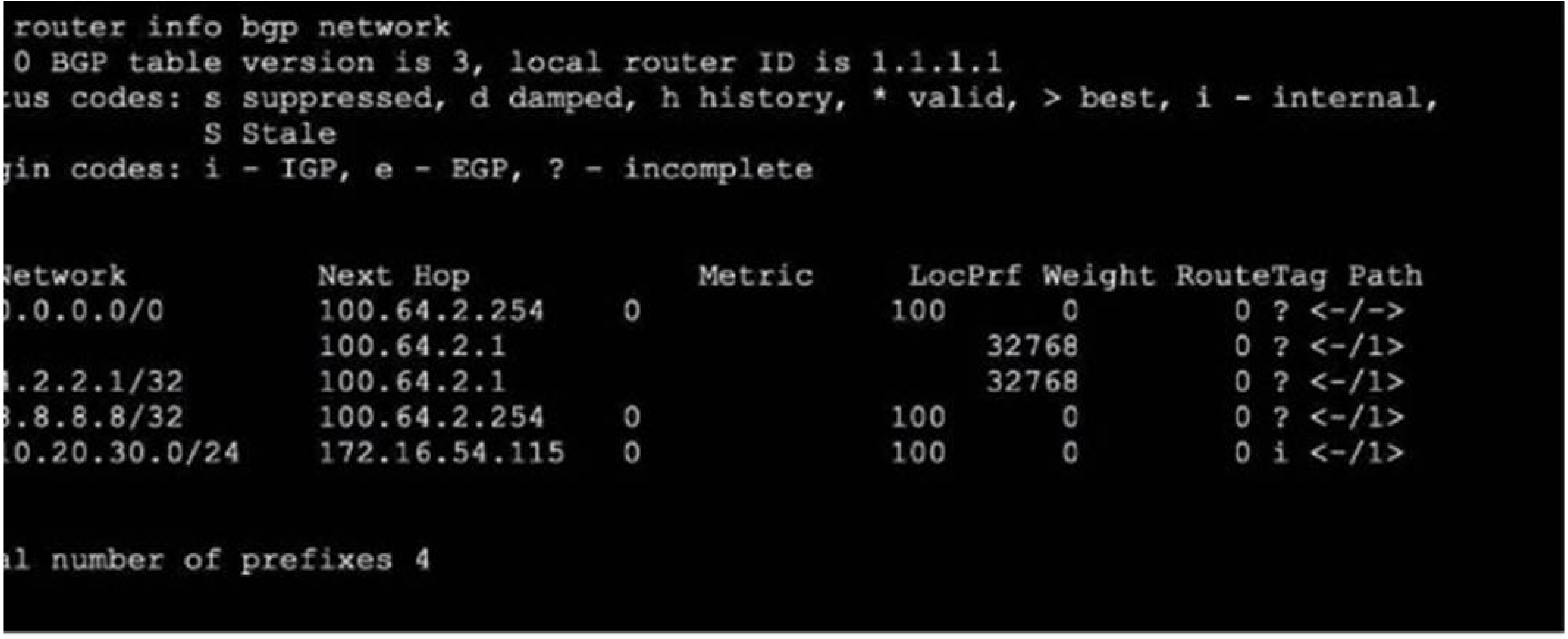
```
# diagnose hardware sysinfo memory
MemTotal:           2055916 kB
MemFree:             708880 kB
Buffers:              22140 kB
Cached:              641364 kB
SwapCached:               0 kB
Active:              726352 kB
Inactive:             98908 kB
```

Refer to the exhibit, which shows a partial output of diagnose hardware aysinfo memory. Which two statements about the output are true? (Choose two.)

A. There are 98908 kB o! memory that will never be used.
B. The user space has 708880 kB of physical memory that is not used by the system.
C. The I/O cache, which has 641364 kB of memory allocated to it.
D. The value indicated next to the inactive heading represents the currently unused cache page.

Answer: AD

NEW QUESTION 9
Refer to the exhibit, which shows the output o! the BGP database.



```
 router info bgp network
 0 BGP table version is 3, local router ID is 1.1.1.1
:us codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           S Stale
gin codes: i - IGP, e - EGP, ? - incomplete


Network          Next Hop            Metric     LocPrf Weight RouteTag Path
).0.0.0/0        100.64.2.254    0              100       0        0 ? <-/->
                 100.64.2.1                           32768        0 ? <-/1>
1.2.2.1/32       100.64.2.1                           32768        0 ? <-/1>
3.8.8.8/32       100.64.2.254    0              100       0        0 ? <-/1>
10.20.30.0/24    172.16.54.115   0              100       0        0 i <-/1>


al number of prefixes 4
```

Which two statements are correct? (Choose two.)

A. The advertised prefix of 10.20.30.0'24 was configured using the network command.
B. The first four prefixes are being advertised using a legacy route advertisement.
C. The advertised prefix of 10.20.30.0'24 is being advertised through the redistribution of another routing protocol.
D. The output shows all prefixes advertised by all neighbors as well as the local router.

Answer: AD

NEW QUESTION 10
......