Fortinet

Exam Questions FCSS_NST_SE-7.6

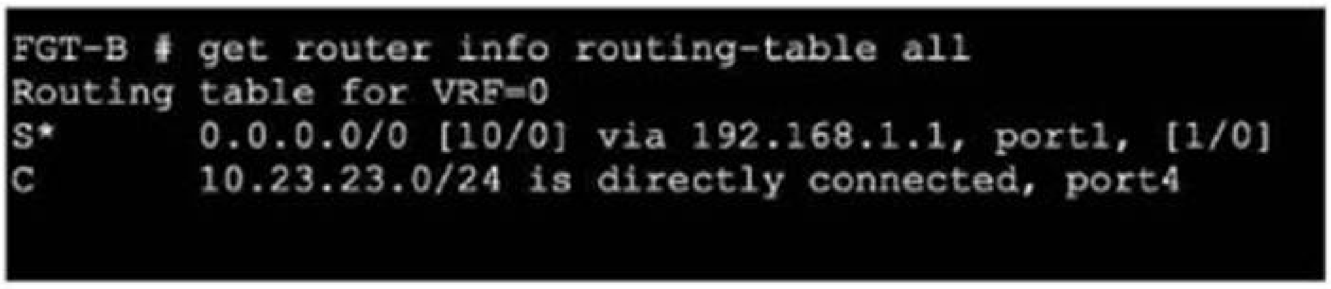
FCSS - Network Security 7.6 Support Engineer

NEW QUESTION 1
In which two slates is a given session categorized as ephemeral? (Choose two.)

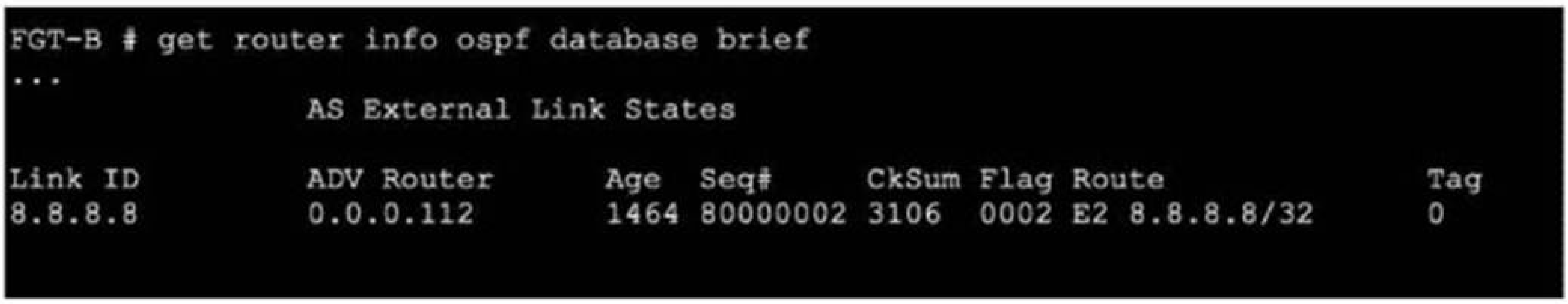
A. A UDP session with only one packet received
B. A UOP session with packets sent and received
C. A TCP session waiting for the SYN ACK
D. A TCP session waiting for FIN ACK

Answer: AC

NEW QUESTION 2
Refer to the exhibits.



```
FGT-B # get router info routing-table all
Routing table for VRF=0
S*       0.0.0.0/0 [10/0] via 192.168.1.1, port1, [1/0]
C        10.23.23.0/24 is directly connected, port4
```



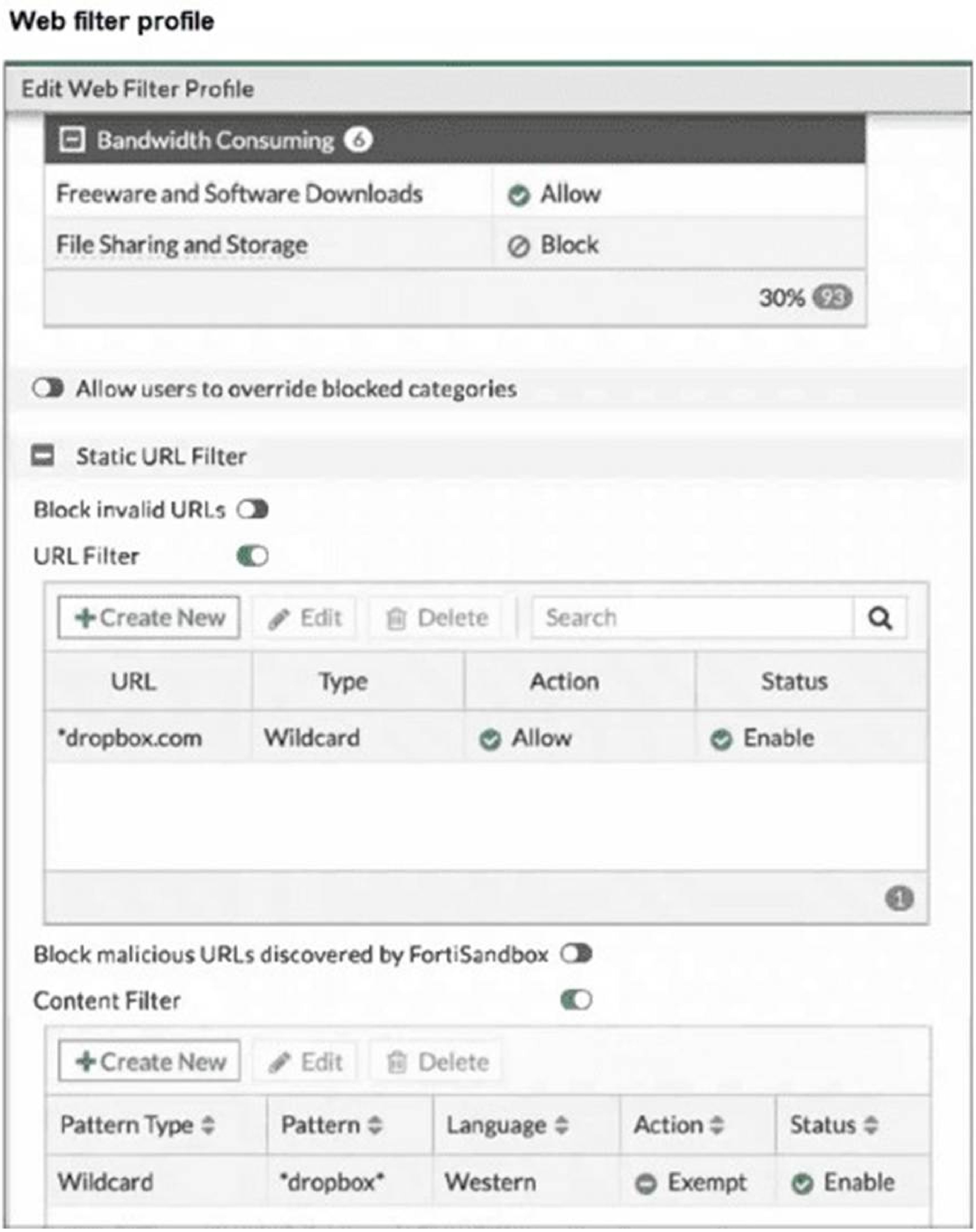
```
FGT-B # get router info ospf database brief
...
                AS External Link States

Link ID         ADV Router       Age  Seq#     CkSum Flag Route              Tag
8.8.8.8         0.0.0.112        1464 80000002 3106  0002 E2 8.8.8.8/32      0
```

An administrator Is expecting to receive advertised route 8.8.8.8/32 from FGT-A. On FGT-B, they confirm that the route is being advertised and received, however, the route is not being injected into the routing table. What is the most likely cause of this issue?

A. A batter route to the 8.8.8.8/32 network exists in the routing table.
B. FGT-B is configured with a prefix list denying the 8.8.8.8/32 network to be injected into the routing table.
C. The administrator has misconfigured redistribution of routes on FGT-A.
D. FGT-8 is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.

Answer: B

NEW QUESTION 3
Refer to the exhibit, which shows a partial web filter profile configuration.



Web filter profile

Edit Web Filter Profile

Bandwidth Consuming 6	
Freeware and Software Downloads	✓ Allow
File Sharing and Storage	⊘ Block
	30% 93

Allow users to override blocked categories

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
*dropbox.com	Wildcard	✓ Allow	✓ Enable

Block malicious URLs discovered by FortiSandbox

Content Filter

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	⊖ Exempt	✓ Enable

The URL www.dropbox.com is categorized as File Sharing and Storage.
Which action does FortiGate take if a user attempts to access www.dropbox.com?

A. FortiGate blocks the connection as an invalid URL.
B. Based on the URL Filter configuration, FortiGate allows the connection.
C. FortiGate blocks the connection, based on the FortiGuard category-based filter configuration.
D. Based on the Web Content filter configuration, access to www.dropbox.com would be exempted.

Answer: B

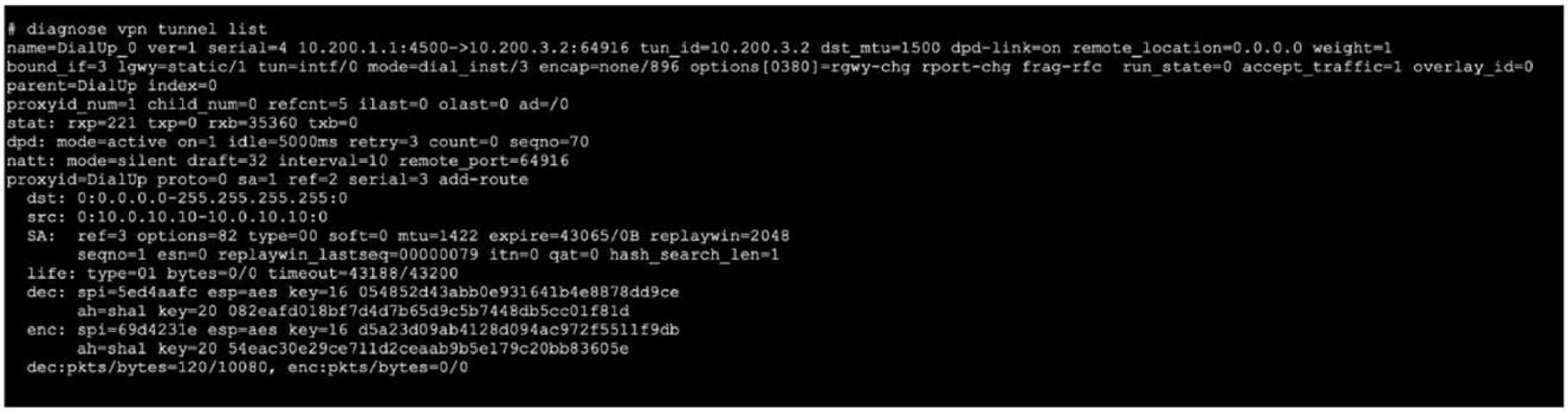
NEW QUESTION 4
Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real-time debug? (Choose three.)

A. Log is full on the collector agent.
B. Inability to reach IP address of the collector agent.

C. Refused connectio
D. Potential mismatch of TCP port.
E. Mismatched pre-shared password.
F. Incompatible collector agent software version.

Answer: BCD

NEW QUESTION 5
Refer to the exhibit, which contains the output of diagnose vpn tunnel list.



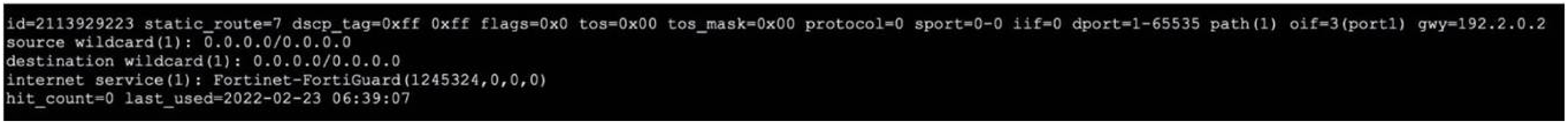
```
# diagnose vpn tunnel list
name=DialUp_0 ver=1 serial=4 10.200.1.1:4500->10.200.3.2:64916 tun_id=10.200.3.2 dst_mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc  run_state=0 accept_traffic=1 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 6
Refer to the exhibit, which shows the output of a policy route table entry.



```
id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
```

Which type of policy route does the output show?

A. An ISDB route
B. A regular policy route
C. A regular policy route, which is associated with an active static route in the FIB
D. An SD-WAN rule

Answer: A

NEW QUESTION 7
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 'Ip proto 50'
C. diagnose sniffer packet any 'udp port 4500'
D. diagnose sniffer packet any 'ah'

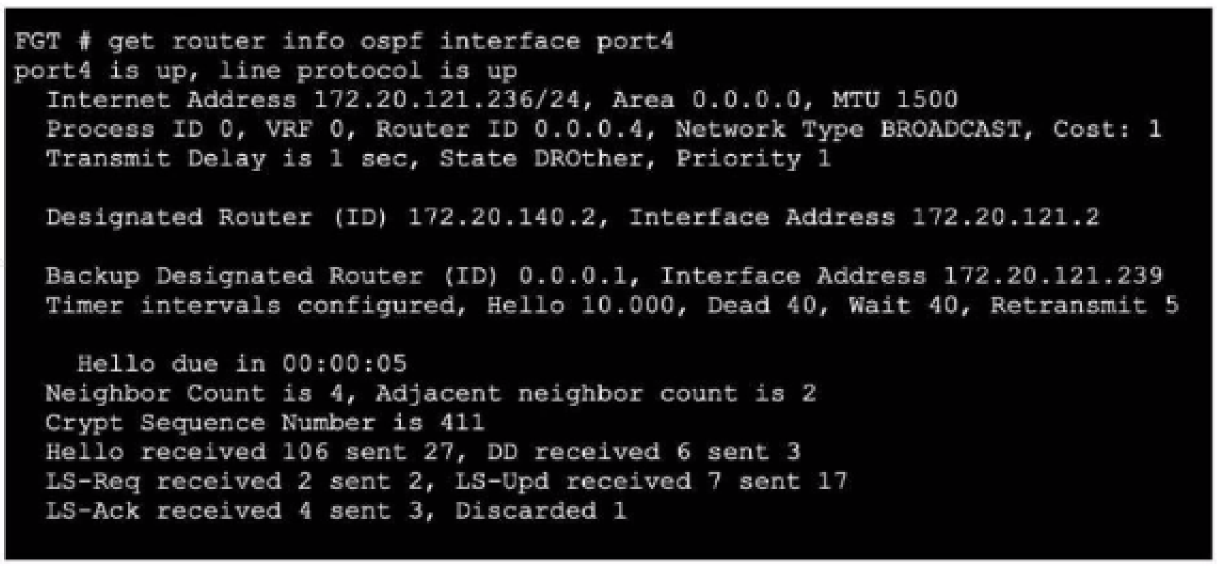
Answer: B

NEW QUESTION 8
Which statement about protocol options is true?

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

NEW QUESTION 9
Refer to the exhibit, which shows the output of a 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: AB

Explanation:
FortiOS Admin Guide: OSPF, Debug Outputs

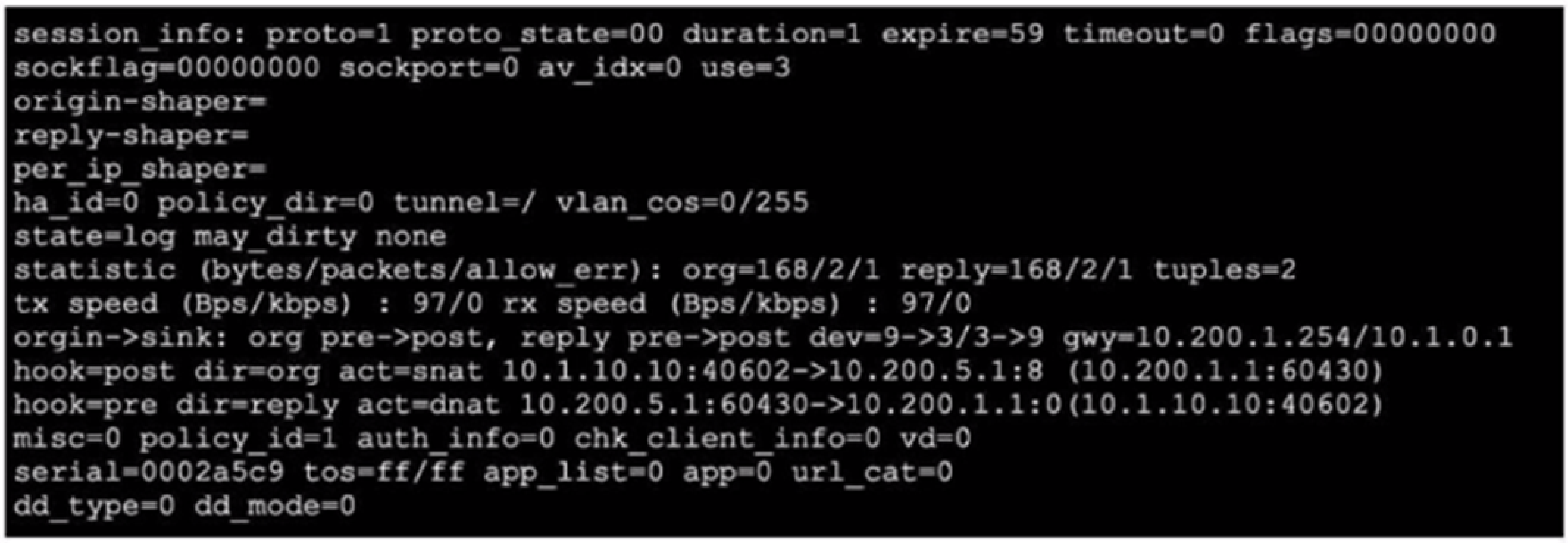
NEW QUESTION 10
Which exchange lakes care of DoS protection in IKEv2?

A. Create_CHILD_SA
B. IKE_Auth
C. IKE_Req_INIT
D. IKE_SA_NIT

Answer: C

Explanation:
TheIKE_SA_INITexchange in IKEv2 is responsible for DoS protection measures. During IKE_SA_INIT, before authentication and further exchange, the responder can use cookie challenges (per RFC 7296 and Fortinet VPN documentation). If a DoS attack is suspected (many requests from the same source), the responder replies with a cookie. Only after the initiator returns the correct cookie does the exchange proceed, protecting the responder from state exhaustion and certain forms of DoS traffic at the handshake stage.
FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections
IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

NEW QUESTION 10
Refer to the exhibit, which shows a session entry.



```
session_info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic (bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed (Bps/kbps) : 97/0 rx speed (Bps/kbps) : 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8 (10.200.1.1:60430)
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement about this session is true?

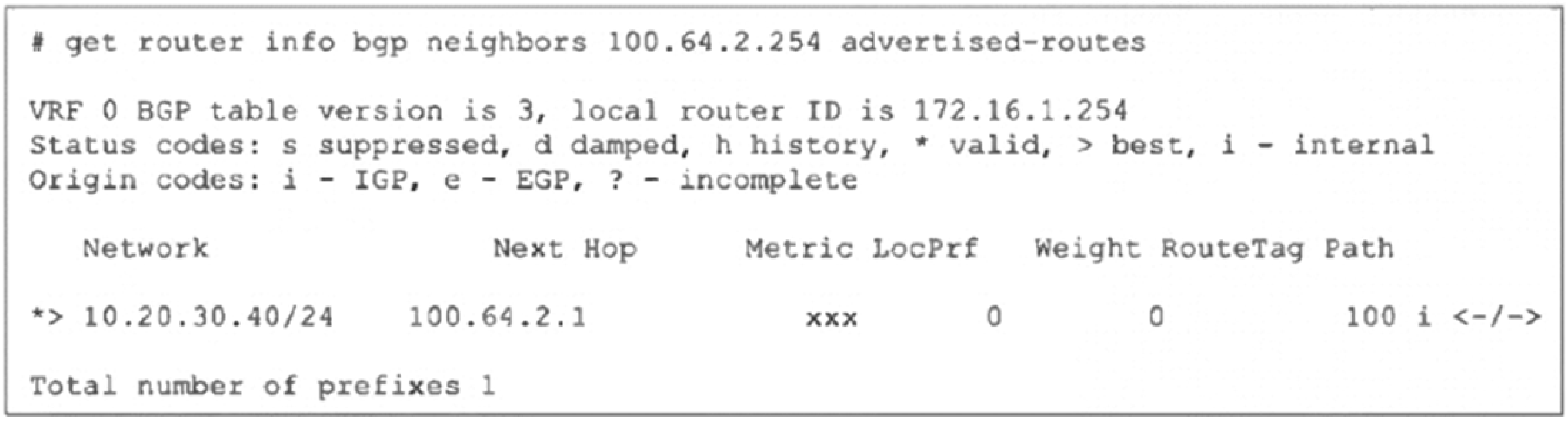
A. Return traffic to the initiator is sent to 10.1.0.1.
B. Return traffic to the initiator is sent lo 10.200.1.254.
C. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.1 to 10.200.5.1.

Answer: B

Explanation:
The session output reveals a session with proto=1 (ICMP) and the origin and reply directions show address and NAT translations. Specifically, thehook=post dir=org act=snatshows that source NAT is performed for outgoing packets, where the source 10.1.10.10:40602 is translated to 10.200.5.1:8 (likely ICMP id 8, not a

TCP/UDP port). The reply direction,hook=pre dir=reply act=dnat, indicates destination NAT for incoming packets: packets incoming for 10.200.5.1:60430 are destination-NATed to 10.1.10.10:40602. The gateway (gwy) is listed as 10.200.1.254/10.1.0.1, which for outgoing traffic means that return traffic is directed to the gateway (10.200.1.254), per the NAT policy. This is confirmed by the FortiOS Session Table Guide, which explains that the returned ICMP reply will be routed out to this NAT gateway. The session statistics and logical flow (SNAT out, matching DNAT in) reinforce that reply traffic to the initiator traverses via 10.200.1.254.
FortiOS Administration Guide: Session Table, NAT, and Route Interaction
Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

NEW QUESTION 15
Refer to the exhibit, which shows the output of the command get router info bgp neighbors 100.64.2.254 advertised-routes.



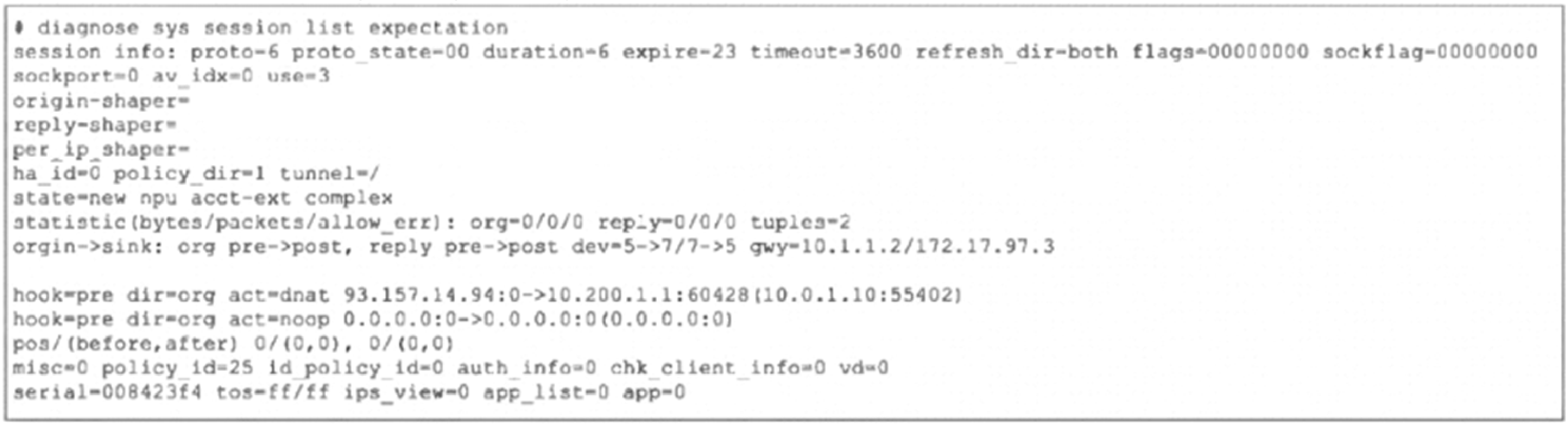
```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop        Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24     100.64.2.1          xxx       0         0           100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

A. The BGP state of the two BGP participants is OpenConfirm.
B. The router ID of the neighbor is 100.64.2.254.
C. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
D. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.

Answer: D

NEW QUESTION 20
Refer to the exhibit, which shows the partial output of a diagnose command.



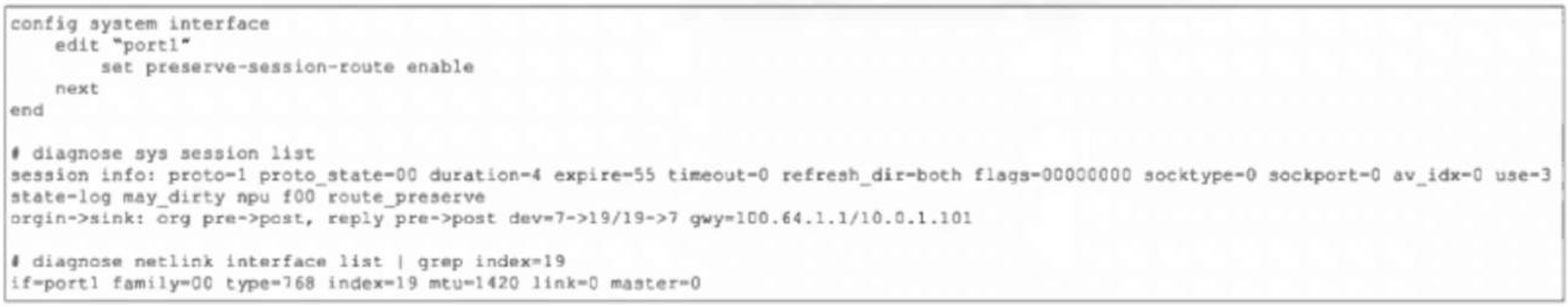
```
# diagnose sys session list expectation
session info: proto=6 proto_state=00 duration=6 expire=23 timeout=3600 refresh_dir=both flags=00000000 sockflag=00000000
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new npu acct-ext complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=5->7/7->5 gwy=10.1.1.2/172.17.97.3

hook=pre dir=org act=dnat 93.157.14.94:0->10.200.1.1:60428(10.0.1.10:55402)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=25 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=008423f4 tos=ff/ff ips_view=0 app_list=0 app=0
```

Which two conclusions can you draw from the output shown in the exhibit? (Choose two.)
A. FortiGate will drop the expected traffic if it does not arrive within 23 seconds.
B. Clearing the master session has no impact on the expectation session.
C. This is a pinhole session to allow traffic for a TCP protocol that dynamically assigns TCP ports.
D. The session is checked against firewall policy ID 25.

A.

Answer: AC

NEW QUESTION 21
Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.



```
config system interface
    edit "port1"
        set preserve-session-route enable
    next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state=log may_dirty npu f00 route_preserve
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 link=0 master=0
```

What happens to the session information if a routing change occurs that affects this session?
A. Only the interface and gateway information for dev=7 will be removed.
B. The session information will not change unless the current route has been removed from the routing table.
C. The session will be flagged as dirty but no route lookups will be performed.

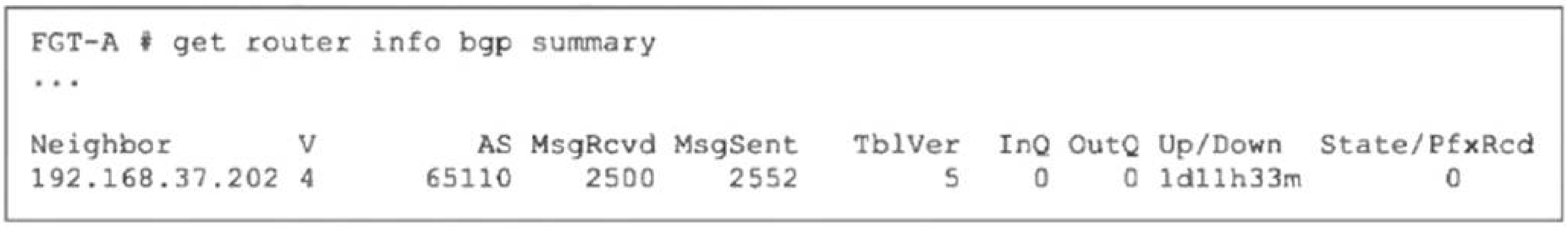
D. Sessions involving port7 or port19 will not have their routing information flushed.

A.

Answer: B

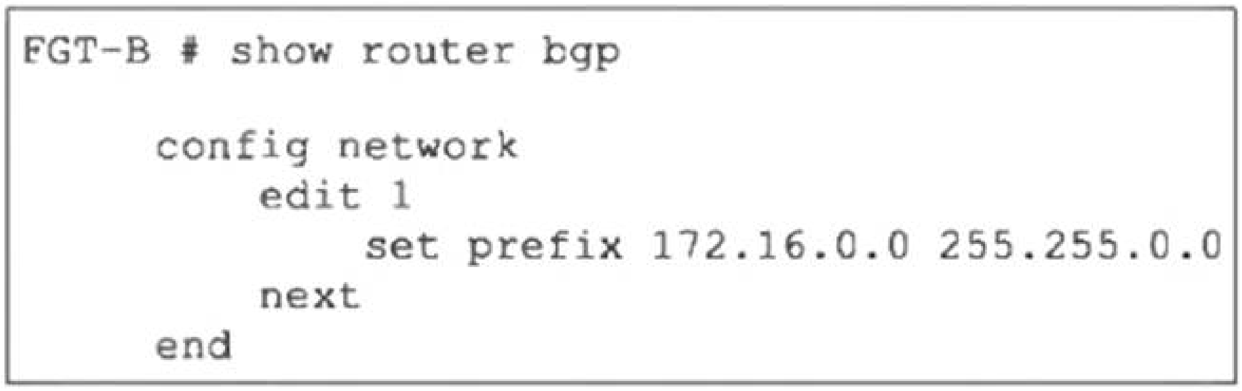
NEW QUESTION 23
Refer to the exhibits.

Exhibit 1



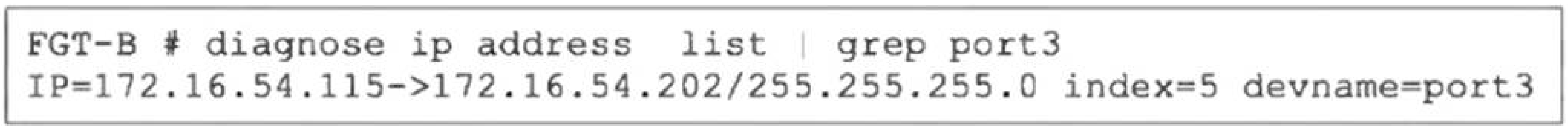
```
FGT-A # get router info bgp summary
...

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4       65110    2500    2552        5    0    0 1d11h33m           0
```

Exhibit 2



```
FGT-B # show router bgp

     config network
         edit 1
             set prefix 172.16.0.0 255.255.0.0
         next
     end
```

Exhibit 3



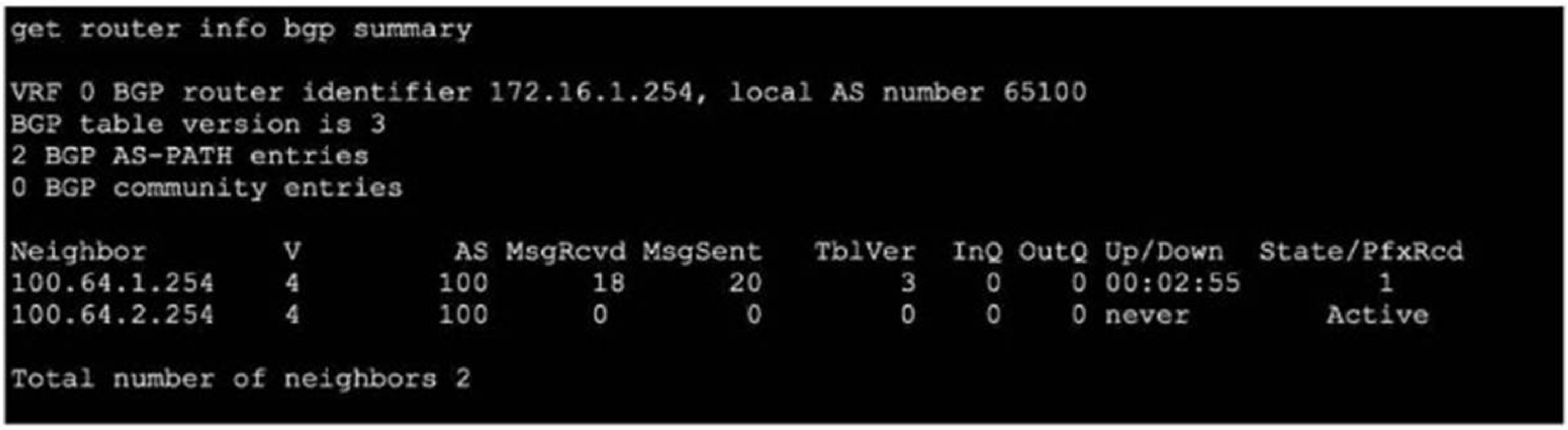
```
FGT-B # diagnose ip address  list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.
Which two actions can the administrator take to fix this problem? (Choose two.)

A. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.
B. Manually add the BGP route on FGT-A.
C. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.
D. Use the set network-import-check disable command.

Answer: AD

NEW QUESTION 28
Refer to the exhibit, which shows the output of get router info bgp summary.



```
get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.64.1.254    4        100      18      20        3    0    0 00:02:55        1
100.64.2.254    4        100       0       0        0    0    0 never          Active

Total number of neighbors 2
```

Which two statements are true? (Choose two.)

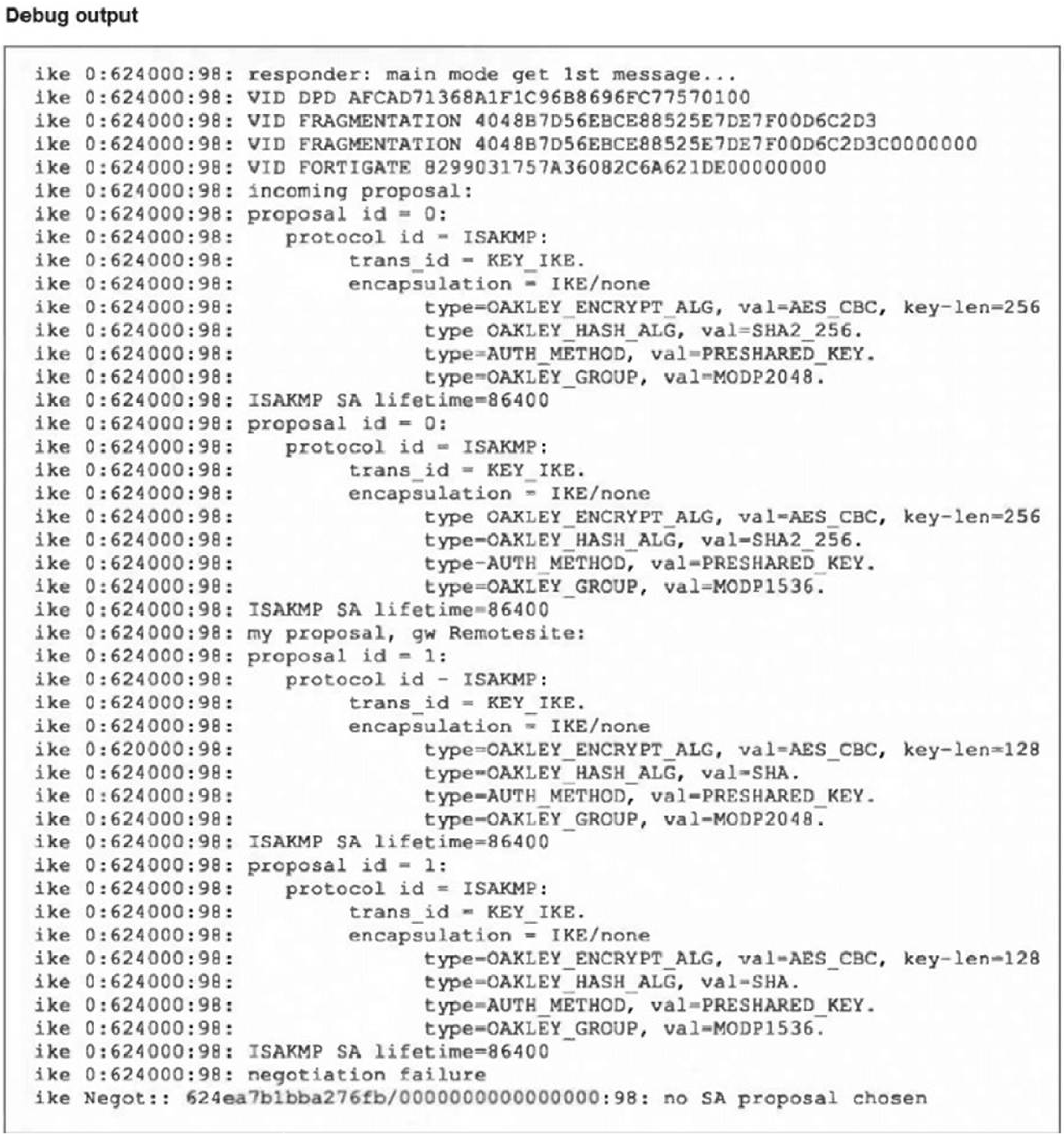
A. The local ForliGate has received one prefix from BGP neighbor 100.64.1.254.
B. The TCP connection with BGP neighbor 100.64.2.254 was successful.
C. The local FortiGate has received 18 packets from a BGP neighbor.
D. The local FortiGate is still calculating the prefixes received from BGP neighbor 100.64.2.264

Answer: AC

Explanation:

The get router info bgp summary output lists BGP neighbor status:
Prefix Reception: The "State/PfxRcd" column shows the number of prefixes received from the neighbor—neighbor 100.64.1.254 has "1", confirming option A.
Received Message Count: Under "MsgRcvd", 18 packets have been received from neighbor 100.64.1.254. This matches option C.
The second neighbor 100.64.2.254 is in "Active" state and has received/sent 0 packets, indicating that its TCP connection is NOT established, disproving option B.
There is no indication anywhere that the router is "still calculating" prefixes; "Active" just means no session is established, so option D is incorrect.
[References:, , FortiOS BGP Command Reference: BGP Neighbor States, PfxRcd, and Counters]

NEW QUESTION 30
Refer to the exhibit, which contains partial output from an IKE real-time debug.



Debug output

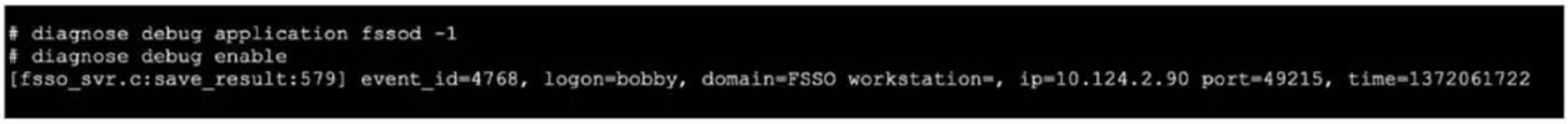
```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:               type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:               type OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:               type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:               type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:               type OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:               type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:               type-AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:               type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id - ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:620000:98:               type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:               type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:               type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:               type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:               type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:               type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:               type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:               type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:: 624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.
Based on the debug output, which configuration change the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.
B. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
C. In the phase 1 network configuration, set the IKE version to 2.
D. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

Answer: A

NEW QUESTION 34
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
```

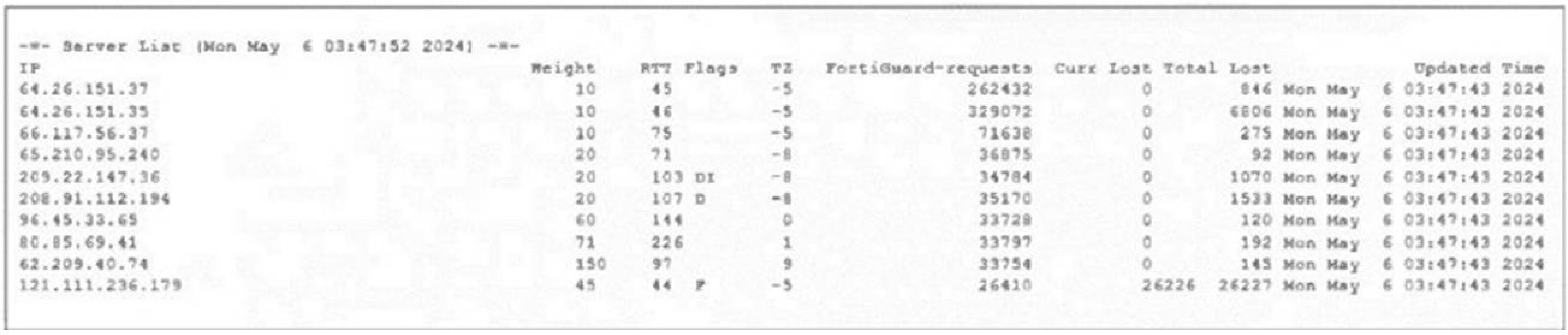
What two conclusions can you draw from the output? (Choose two.)

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

Explanation:
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349
From the snippet we can see that FortiGate (via the fssod daemon) is directly detecting the user logon rather than relying on a separate ??collector?? or ??DC agent.?? This indicates agentless polling—FortiGate polls the DC??s event logs over TCP 445 to discover logons. So: - FSSO is using agentless polling mode to detect logon events - In agentless mode, FortiGate will periodically poll the same IP (the DC) on port 445 to see if the user is still logged on

NEW QUESTION 39
Refer to the exhibit, which shows the partial output of command diagnose debug rating.

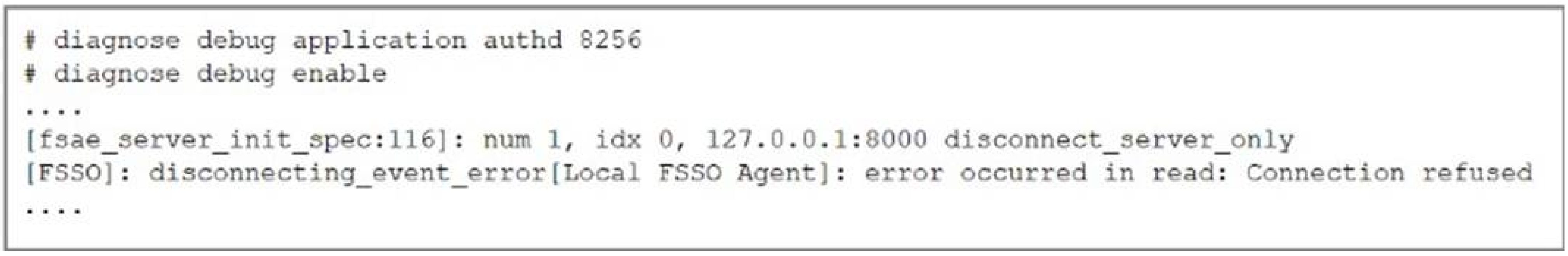


```
-=- Server List (Mon May  6 03:47:52 2024) -=-
IP                                  Weight   RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost            Updated Time
64.26.151.37                            10    45         -5                262432          0        846 Mon May  6 03:47:43 2024
64.26.151.35                            10    46         -5                329072          0       6806 Mon May  6 03:47:43 2024
66.117.56.37                            10    75         -5                 71638          0        275 Mon May  6 03:47:43 2024
65.210.95.240                           20    71         -8                 36875          0         92 Mon May  6 03:47:43 2024
209.22.147.36                           20   103 DI      -8                 34784          0       1070 Mon May  6 03:47:43 2024
208.91.112.194                          20   107 D       -8                 35170          0       1533 Mon May  6 03:47:43 2024
96.45.33.65                             60   144          0                 33728          0        120 Mon May  6 03:47:43 2024
80.85.69.41                             71   226          1                 33797          0        192 Mon May  6 03:47:43 2024
62.209.40.74                           150    97          9                 33754          0        145 Mon May  6 03:47:43 2024
121.111.236.179                         45    44  F      -5                 26410      26226      26227 Mon May  6 03:47:43 2024
```

A. 66.117.56.37
B. 208.91.112.194
C. 209.22.147.36
D. 64.26.151.37

Answer: D

NEW QUESTION 42
Refer to the exhibit showing a debug output.



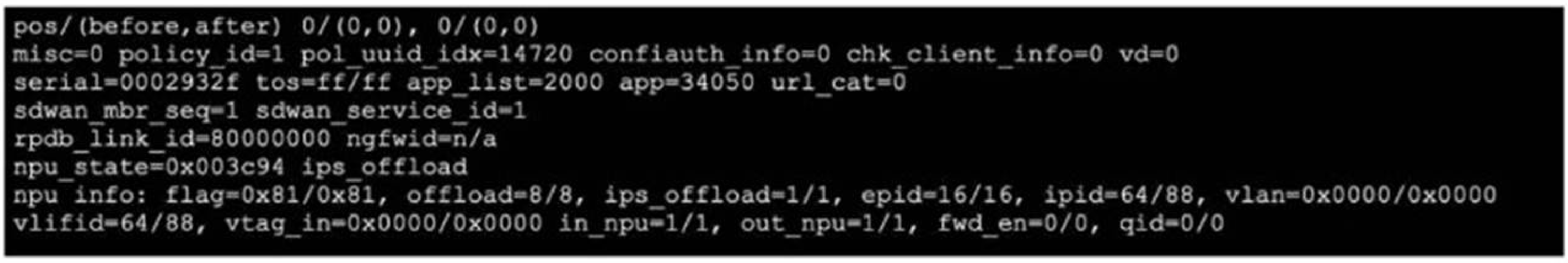
```
# diagnose debug application authd 8256
# diagnose debug enable
....
[fsae_server_init_spec:116]: num 1, idx 0, 127.0.0.1:8000 disconnect_server_only
[FSSO]: disconnecting_event_error[Local FSSO Agent]: error occurred in read: Connection refused
....
```

An administrator deployed FSSO in DC Agent Mode but FSSO is failing on FortiGate. Pinging FortiGate from where the collector agent is deployed is successful. The administrator then produces the debug output shown in the exhibit.
What could be causing this error message?

A. The TCP port 445 is blocked between FortiGate and collector agent.
B. The collector agent preshared password is mismatched.
C. The FortiGate cannot resolve the active directory server name.
D. The FortiGate and the collector agent are using different TCP ports.

Answer: D

NEW QUESTION 45
Refer to the exhibit, which shows the omitted output of a session table entry.



```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

Which two statements are true? (Choose two.)

A. The traffic has been tagged for VLAN 0000.
B. NP7 is handling offloading of this session.
C. The traffic matches Policy ID 1.
D. The session has been offloaded.

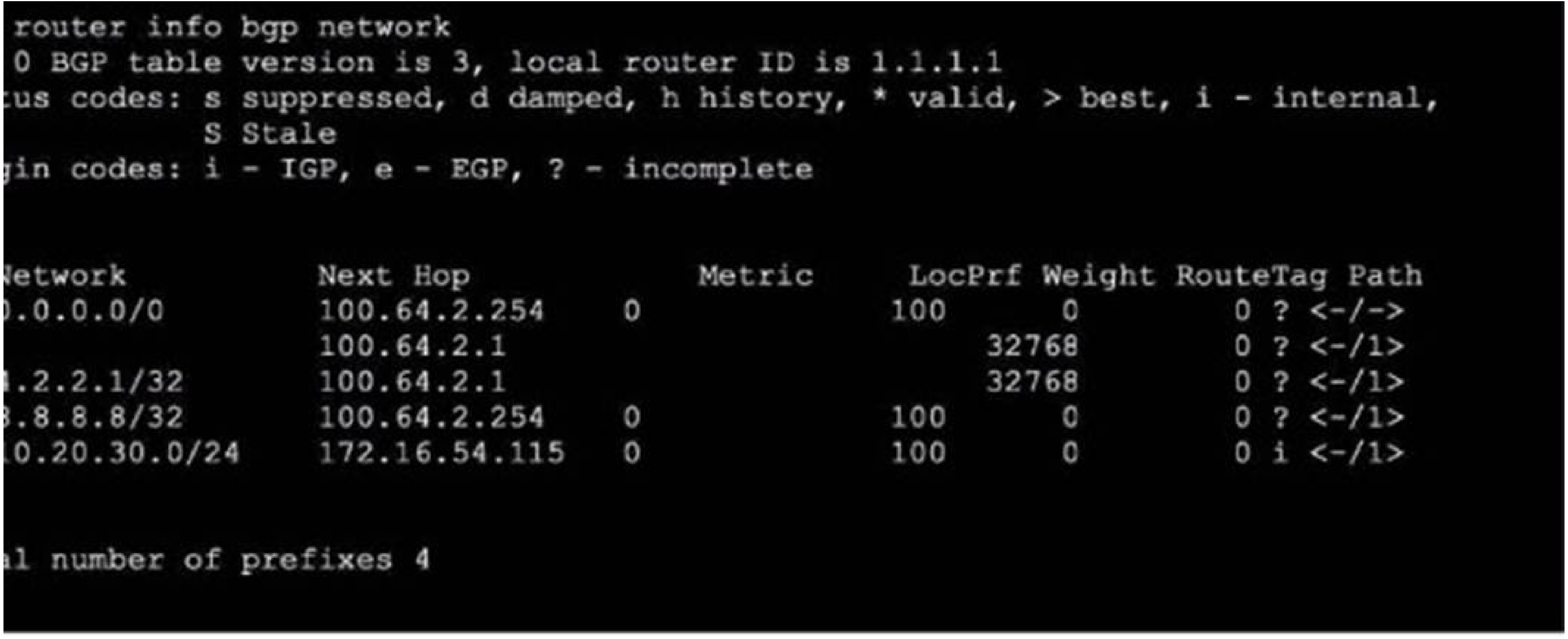
Answer: BD

NEW QUESTION 46
Which two statements about an auxiliary session ate true? (Choose two.)

A. With the auxiliary session selling disabled, only auxiliary sessions are offloaded.
B. With the auxiliary session setting enable
C. ECMP traffic is accelerated to the NP6 processor.
D. With the auxiliary session setting enable
E. Iwo sessions are created in case of routing change.
F. With the auxiliary session setting disabled, for each traffic pat
G. FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 51
Refer to the exhibit, which shows the output o! the BGP database.



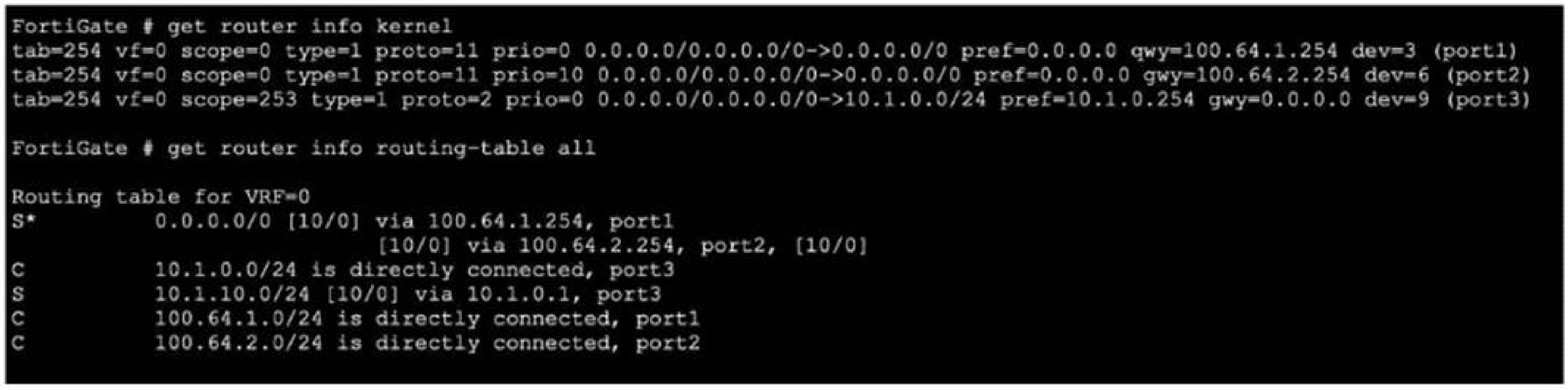
```
 router info bgp network
 0 BGP table version is 3, local router ID is 1.1.1.1
:us codes: s suppressed, d damped, h history, * valid, > best, i - internal,
             S Stale
jin codes: i - IGP, e - EGP, ? - incomplete


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>
..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>
l0.20.30.0/24    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 53
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?

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

NEW QUESTION 55

What are two functions of automation stitches? (Choose two.)

A. You can configure automation stitches on any FortiGate device in a Security Fabric environment.
B. You can configure automation stitches to execute actions sequentially by taking parameters from previous actions as input for the current action.
C. You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.
D. You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

Answer: BD

NEW QUESTION 58

......