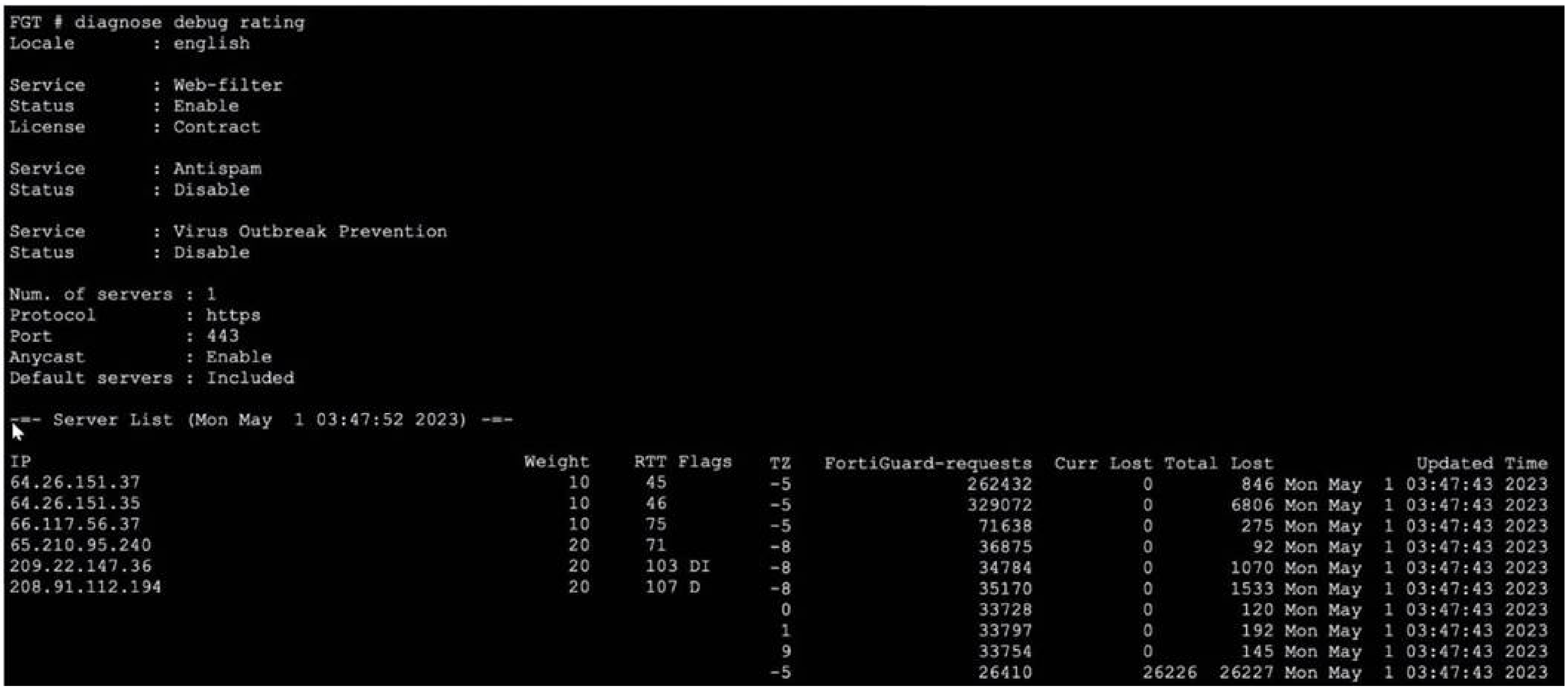
Fortinet

Exam Questions FCSS_NST_SE-7.4

FCSS - Network Security 7.4 Support Engineer

NEW QUESTION 1
Exhibit.



```
FGT # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Mon May  1 03:47:52 2023) -=-

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  1 03:47:43 2023
64.26.151.35                                       10     46          -5                 329072         0       6806 Mon May  1 03:47:43 2023
66.117.56.37                                       10     75          -5                  71638         0        275 Mon May  1 03:47:43 2023
65.210.95.240                                      20     71          -8                  36875         0         92 Mon May  1 03:47:43 2023
209.22.147.36                                      20     103 DI      -8                  34784         0       1070 Mon May  1 03:47:43 2023
208.91.112.194                                     20     107 D       -8                  35170         0       1533 Mon May  1 03:47:43 2023
                                                                       0                  33728         0        120 Mon May  1 03:47:43 2023
                                                                       1                  33797         0        192 Mon May  1 03:47:43 2023
                                                                       9                  33754         0        145 Mon May  1 03:47:43 2023
                                                                      -5                  26410     26226  26227 Mon May  1 03:47:43 2023
```

Refer to the exhibit, which shows the output of a diagnose command. What can you conclude about the debug output in this scenario?

A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.
B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.
C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
D. Servers with a negative TZ value are less preferred for rating requests.

Answer: B

NEW QUESTION 2
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 3
Which statement about IKEv2 is true?

A. Both IKEv1and IKEv2 share the feature of asymmetric authentication.
B. IKEv1and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.
C. IKEv1and IKEv2 use same TCP port but run on different UDP ports.
D. IKEv1and IKEv2 share the concept of phase1and phase2.

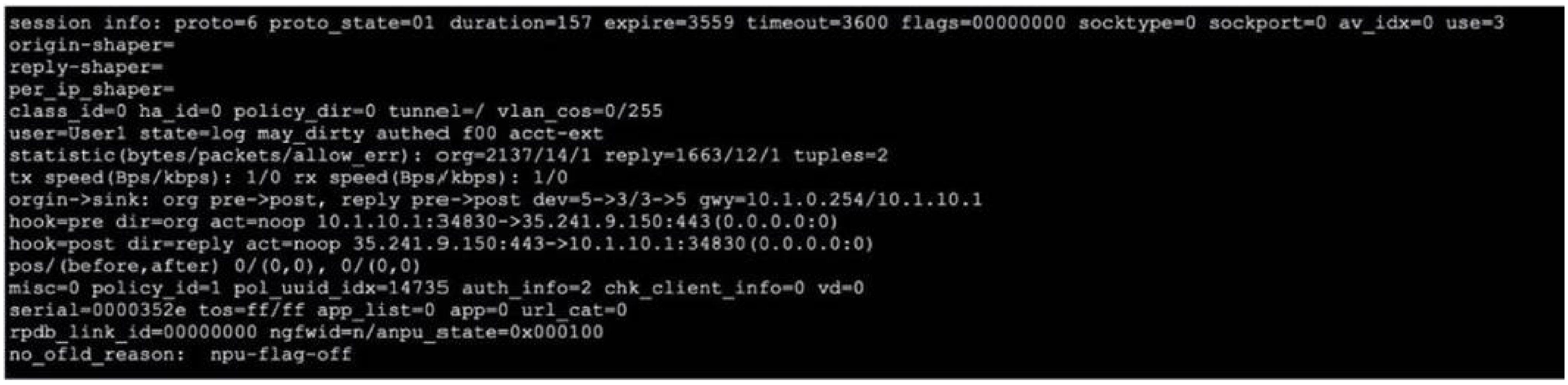
Answer: B

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
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.)

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: AB

NEW QUESTION 6
Which authentication option can you not configure under config user radius on FortiOS?

A. mschap
B. pap
C. mschap2
D. eap

Answer: D

NEW QUESTION 7
Which statement aboutprotocol 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 8
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.

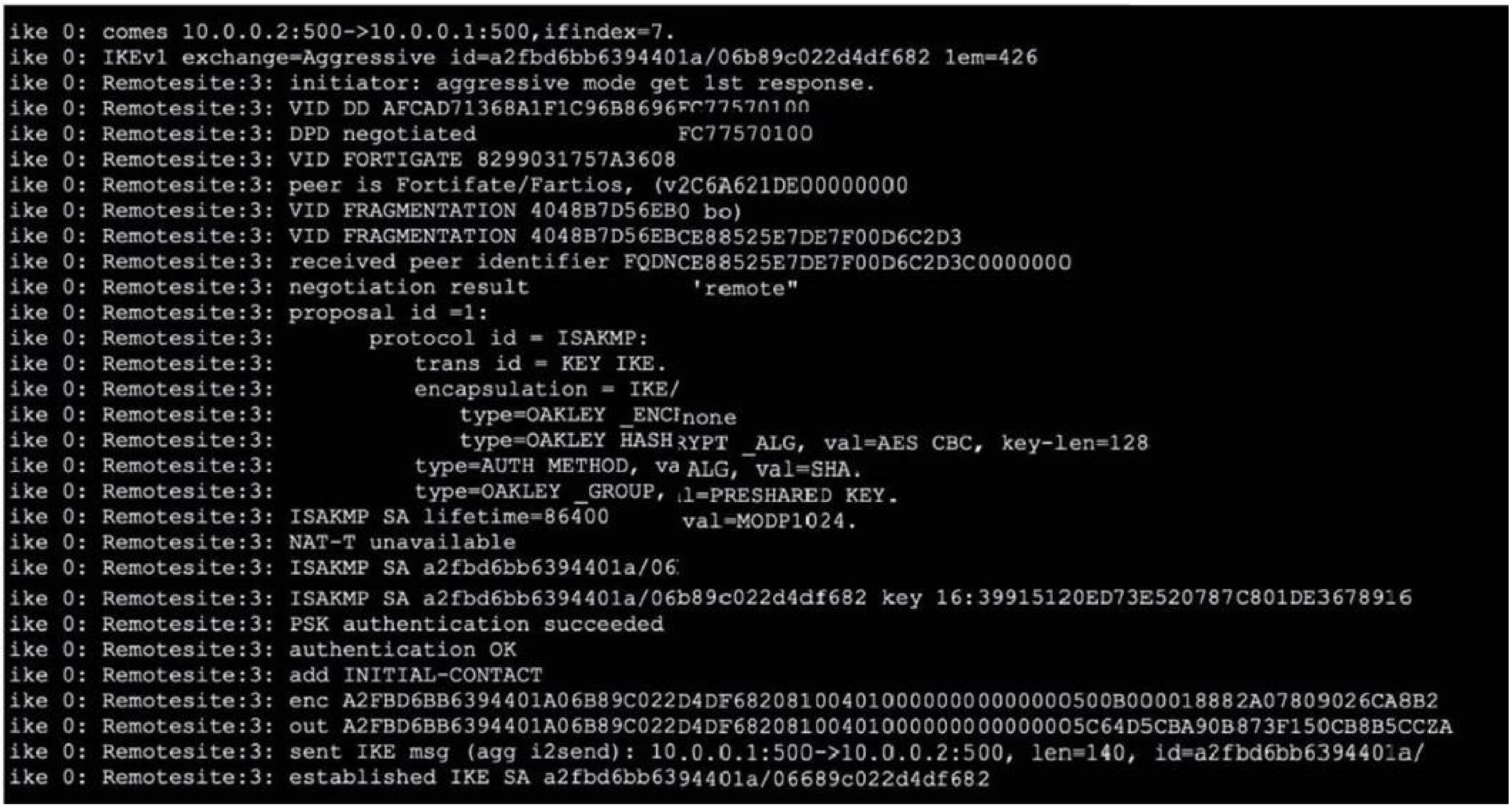
Answer: C

NEW QUESTION 9
Which two statements are true regarding heartbeat messages sent from an FSSO collector agent to FortiGate? (Choose two.)

A. The heartbeat messages can be seen using the command diagnose debug authd fsso list.
B. The heartbeat messages can be seen in the collector agent logs.
C. The heartbeat messages can be seen on FortiGate using the real-lime FSSO debug.
D. The heartbeat messages must be manually enabled on FortiGate.

Answer: BC

NEW QUESTION 10
Exhibit.



```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 lem=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response.
ike 0: Remotesite:3: VID DD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated                FC77570100
ike 0: Remotesite:3: VID FORTIGATE 8299031757A3608
ike 0: Remotesite:3: peer is Fortifate/Fartios, (v2C6A621DE00000000
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EB0 bo)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: received peer identifier FQDNCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: negotiation result              'remote"
ike 0: Remotesite:3: proposal id =1:
ike 0: Remotesite:3:       protocol id = ISAKMP:
ike 0: Remotesite:3:           trans id = KEY IKE.
ike 0: Remotesite:3:           encapsulation = IKE/
ike 0: Remotesite:3:               type=OAKLEY _ENCInone
ike 0: Remotesite:3:               type=OAKLEY HASHRYPT _ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3:           type=AUTH METHOD, va ALG, val=SHA.
ike 0: Remotesite:3:           type=OAKLEY _GROUP, l=PRESHARED KEY.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400      val=MODP1024.
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF682081004010000000000000005C64D5CBA90B873F150CB8B5CCZA
ike 0: Remotesite:3: sent IKE msg (agg i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06689c022d4df682
```

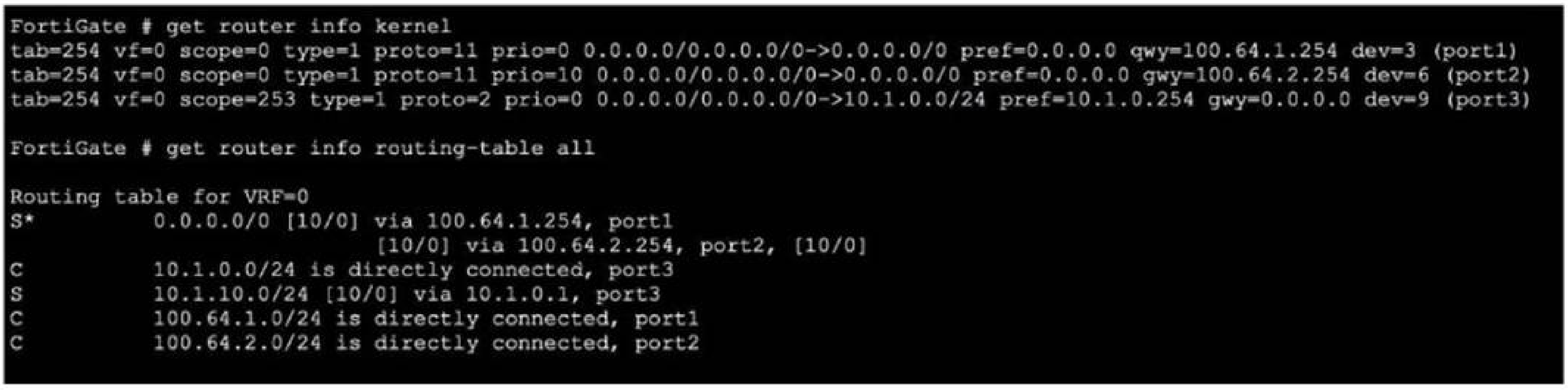
Refer to the exhibit, which contains partial output from an IKE real-time debug. Which two statements about this debug output are correct? (Choose two.)

A. Perfect Forward Secrecy (PFS) is enabled in the configuration.
B. The local gateway IP address is 10.0.0.1.
C. It shows a phase 2 negotiation.
D. The initiator provided remote as its IPsec peer ID.

Answer: CD

NEW QUESTION 10

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 gwy=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
```

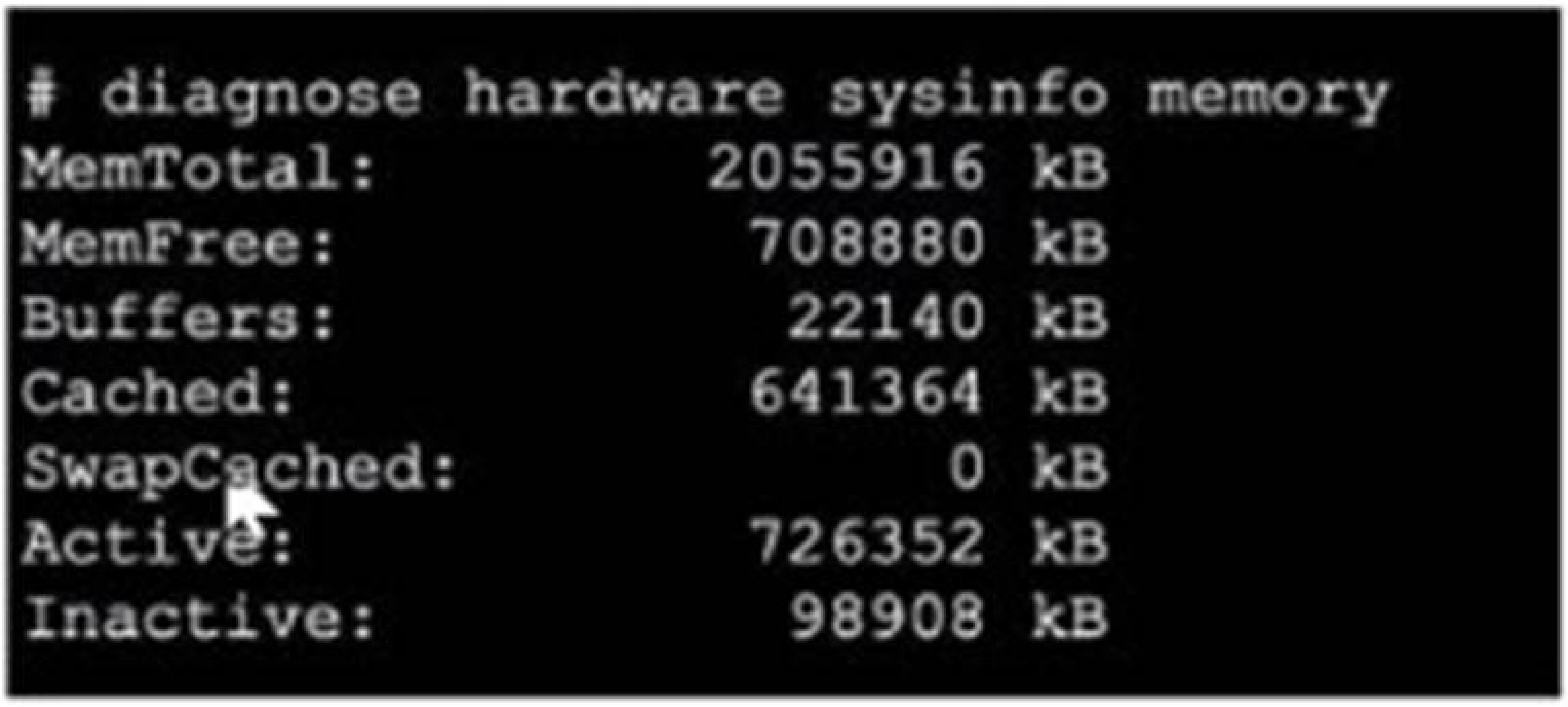
Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

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 11

Exhibit.



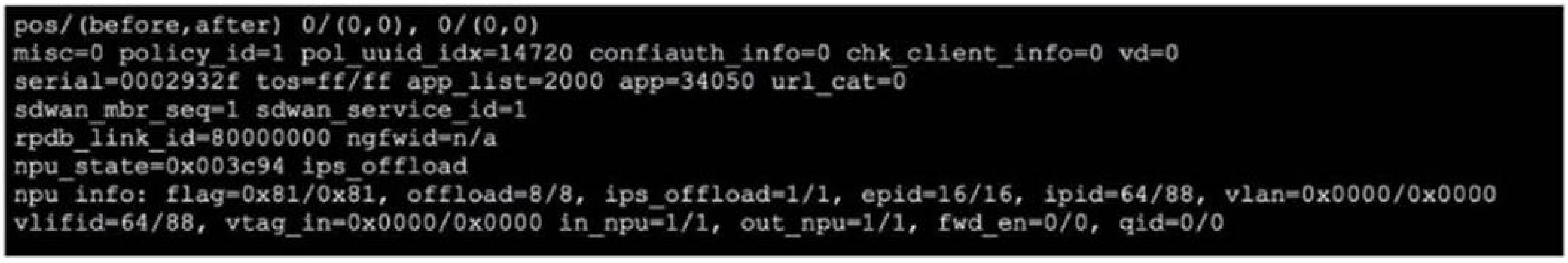
```
# diagnose hardware sysinfo memory
MemTotal:              2055916 kB
MemFree:                708880 kB
Buffers:                 22140 kB
Cached:                 641364 kB
SwapCached:                  0 kB
Active:                 726352 kB
Inactive:                98908 kB
```

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 15
Refer to the exhibit, which shows the omitted output of a session table entry.



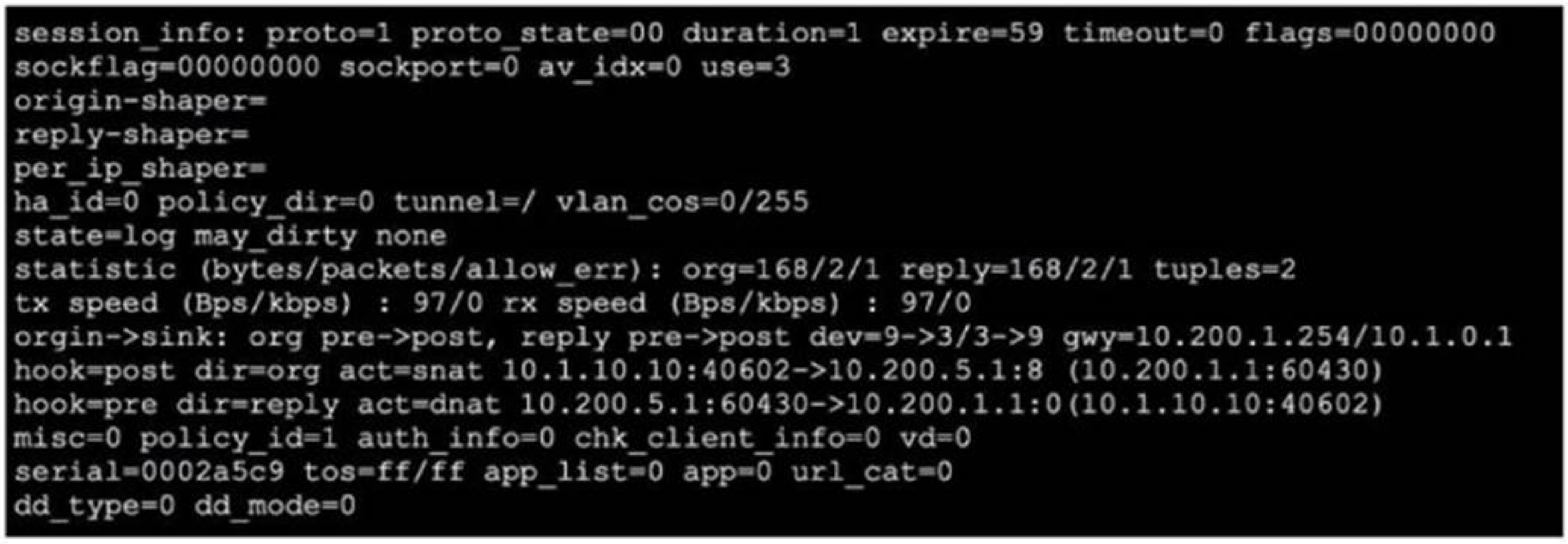
```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, 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 17
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: D

NEW QUESTION 19
Which two statements about Security Fabric communications are true? (Choose two.)

A. FortiTelemetry and Neighbor Discovery both operate using TCP.
B. The default port for Neighbor Discovery can be modified.
C. FortiTelemetry must be manually enabled on the FortiGate interface.
D. By default, the downstream FortiGate establishes a connection with the upstream FortiGate using TCP port 8013.

Answer: CD

NEW QUESTION 23
......