QUESTION 33
In which two slates is a given session categorized as ephemeral? (Choose two.)

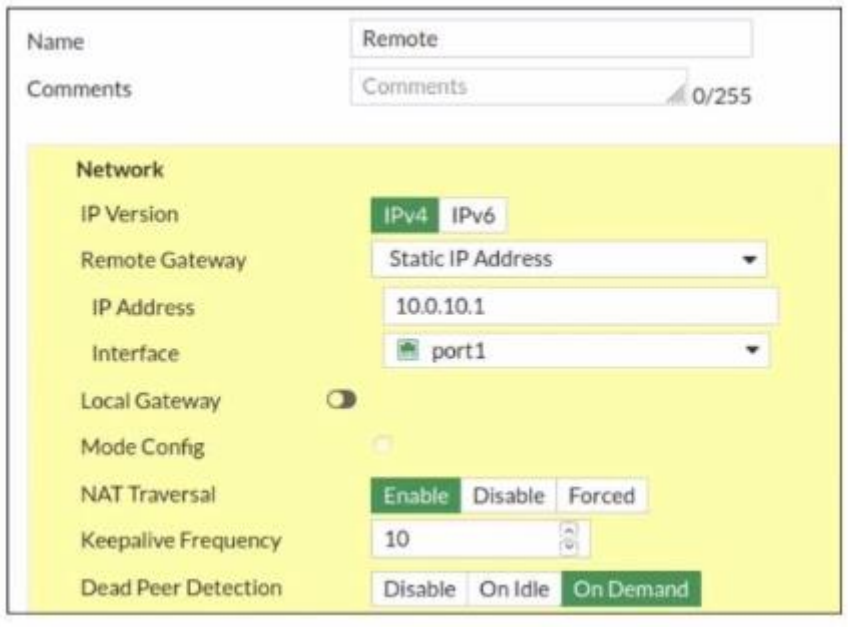
A. A UDP session with only one packet received
B. A UOP session with packets sent and received
C. A TCP session waiting for the SYN ACK
D. A TCP session waiting for FIN ACK

Answer: AC

QUESTION 34
Refer to the exhibit, which contains a screenshot of some phase 1 settings. The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands on an SSH session on FortiGate:

```
diagnose vpn ike log-filter dst-addr4 10.0.10.1
diagnose debug application ike -1
```

However, the IKE real-time debug does not show any output. Why?



A. The administrator must also run the command diagnose debug enable.
B. The debug shows only error messages. If there is no output, then the phase 1 and phase 2 configurations match.
C. The log-filter setting is incorrect. The VPN traffic does not match this filter.
D. Replace diagnose debug application ike -1 with diagnose debug application ipsec -1.

Answer: A

QUESTION 35
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

QUESTION 36
Refer to the exhibit, which shows a truncated output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -1
# diagnose debug enable
   fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
   fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
   fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
   fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
   fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
   fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

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

A. The name of the configured LDAP server is Lab.
B. The user is authenticating using CN=John Smith.
C. FortiOS is able to locate the user in step 3 (Bind Request) of the LDAP authentication process.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: BD

QUESTION 37
Refer to the exhibit, which shows a session entry.


```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=1 expire=3599 timeout=3600 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 us
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 app_valid
statistic(bytes/packets/allow_err): org=1720/9/1 reply=10804/13/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->31/31->7 gwy=10.1.0.254/10.9.31.117
hook=post dir=org act=snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)
hook=pre dir=reply act=dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)
hook=post dir=reply act=noop 200.8.57.5:443->10.9.31.117:45388(0.0.0.0:0)
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 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: A
Explanation:
Return packet routing back to the source follows this format gwy=10.200.1.254 (this is the gateway to the dest) / 10.1.0.1 (this is the destination's gateway back to the source).

QUESTION 38
Which statement about parallel path processing is correct (PPP)?

A. PPP chooses from a group of parallel options lo identity the optimal path tor processing a packet.
B. Only FortiGate hardware configurations affect the path that a packet takes.
C. PPP does not apply to packets that are part of an already established session.
D. Software configuration has no impact on PPP.

Answer: A

QUESTION 39
In IKEv2, which exchange establishes the first CHILD_SA?

A. IKE_SA_INIT
B. INFORMATIONAL
C. CREATE_CHILD_SA
D. IKE_Auth

Answer: C

QUESTION 40
Which authentication option can you not configure under config user radius on FortiOS?

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

Answer: D

QUESTION 41
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
Explanation:
Add an AES256-SHA256 proposal to your local Phase 1 settings so that the FortiGate can match the peer's AES-CBC/256 with SHA-256 proposal.

QUESTION 42
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 connection. Potential mismatch of TCP port.
D. Mismatched pre-shared password.
E. Incompatible collector agent software version.

Answer: BCD
Explanation:
When you enable FSSO real-time debug you'll see explicit socket errors if the FortiGate can't reach the collector's IP (e.g. timeout or "no route to host"), which tells you the agent isn't reachable. If the TCP port is wrong or the listener isn't running, you'll see "Connection refused" in the debug output, pinpointing a port mismatch. And if the configured pre-shared secret doesn't match, the logs show an authentication failure or "invalid key" message, clearly indicating a password mismatch. These three conditions - unreachable IP, refused connection, and bad PSK - are all directly diagnosable via the real-time debug.

QUESTION 43
Refer to the exhibit, which shows a partial output from the get router info routing-table database command.

```
# get router info routing-table database
---omitted---

Routing table for VRF=0
S           0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S           0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive, [50/0]
---omitted---
```

The administrator wants to configure a default static route for port3 and assign a distance of 50 and a priority of 0.
What will happen to the port1 and port2 default static routes after the port3 default static route is created?

A. The port2 default static route will be injected into the forwarding information base (FIB).
B. The port1 default static route will be injected into the FIB.
C. Neither of the routes shown in the output will be injected into the FIB.
D. Both default static routes shown in the output will be injected into the FIB.

Answer: A

Explanation:
After adding the port3 default route (distance 50), the best active route remains the port2 static route (distance 20), so that port2 entry stays installed in the FIB. The port1 route remains inactive and is not installed.

QUESTION 44
The local OSPF router is unable to establish adjacency with a peer. Which two things should the administrator do to troubleshoot the issue? (Choose two.)

A. Check whether TCP port 179 is blocked.
B. Check if there is an active static route to the peer.
C. Check whether both peers have an IP address within the same subnet.
D. Check if IP protocol 89 is blocked.

Answer: CD
Explanation:
Verify that both routers' OSPF-enabled interfaces have IPs in the same subnet - adjacency only forms with peers on the same network segment.
Make sure IP protocol 89 (OSPF) isn't being blocked by any firewall or ACL—OSPF uses IP 89, not a TCP or UDP port.

QUESTION 45
Refer to the exhibit. An IPsec VPN tunnel is dropping, as shown by the debug output. Analyzing the debug output, what could be causing the tunnel to go down?

Debug output

```
FGT # diagnose debug application ike -1

FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b8b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B708100501 9E253B8B0000006CE306FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF6BF6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB000002000000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA9B8204D890A367DBDDDB20E5812CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:b1dd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E38196550041FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD000002000000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A09398EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB96B354FF46B84E6A79622FC1D44BC7F9649864AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A8338000002000000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDDB812D02AE1672BD0E893431344D7BC31E9323A2C56E27DB43B747870885D7954558993B25BC43118695BEA47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

A. Phase 2 drops but Phase 1 is up.
B. Dead Peer Detection is not receiving its acknowledge packet.
C. The tunnel drops during rekey negotiation.
D. The tunnel drops after the timer expires.

Answer: B
Explanation:
The continual "notify msg received: R-U-THERE" without any corresponding DPD response causes the FortiGate to delete the IPsec SA when its Dead Peer Detection timer expires, bringing the tunnel down.

QUESTION 46
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
```

In this exhibit, which FDS server will the FortiGate algorithm choose?

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

Answer: D
Explanation:
The FortiGate will pick 64.26.151.37, since it ties for the lowest weight (10) and has the lowest RTT (45 ms) of all the weight-10 servers.