Number: FCSS_NST_SE-7.4
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: FCSS_NST_SE-7.4

Exam Name: FCSS - Network Security 7.4 Support Engineer

Exam A

QUESTION 1
Exhibit.

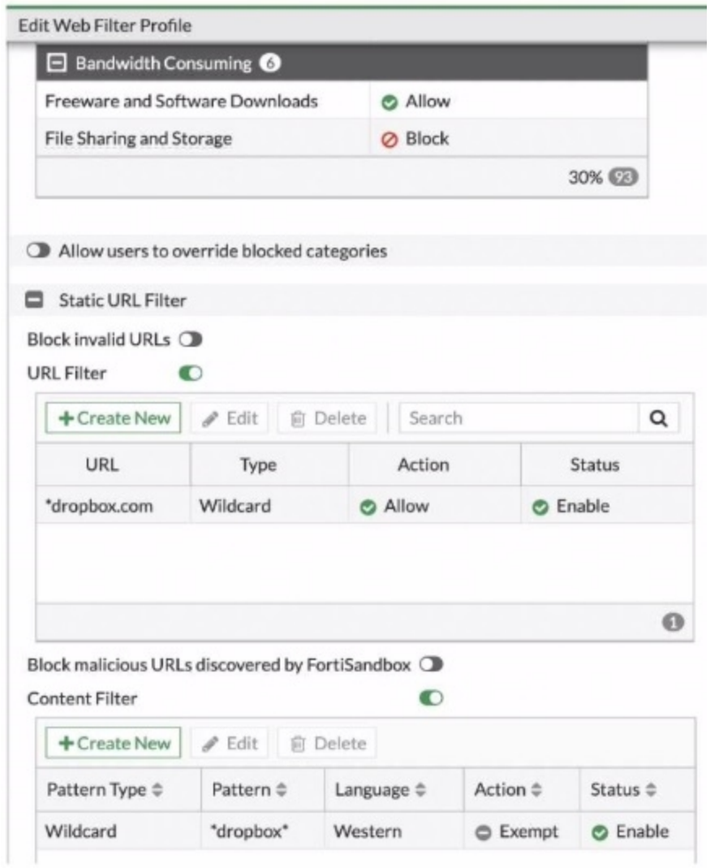
```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
   <2023/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
    FGVM010000077649(updated 4 seconds ago): in-sync
    FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
    FGVM010000077649(updated 4 seconds ago):
        sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
    FGVM010000077650(updated 1 seconds ago):
        sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
    FGVM010000077649(updated 4 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
    FGVM010000077650(updated 1 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary     : NGFW-1          , FGVM010000077649, HA cluster index = 1
Secondary   : NGFW-2          , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

Refer to the exhibit, which shows the output of get system ha status.
NGFW-1 and NGFW-2 have been up for a week.
Which two statements about the output are true? (Choose two)

A. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.
B. If port 7 becomes disconnected on the secondary, both FortiGate devices will elect itself as primary.
C. If FGVM...649 is rebooted. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
D. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

Correct Answer: B, C
Section:

QUESTION 2
Exhibit.



Refer to the exhibit, which shows a partial web fillet profile configuration.
Which action does FortiGate lake if a user attempts to access www. dropbox. com, which is categorized as File Sharing and Storage?

A. FortiGate allows the connection, based on the URL Filter configuration.
B. FortiGate blocks the connection as an invalid URL.
C. FortiGate exempts the connection, based on the Web Content Filter configuration.
D. FortiGate blocks the connection, based on the FortiGuard category based filter configuration.

Correct Answer: D
Section:

QUESTION 3
Refer to the exhibit, which shows the omitted output of a session table entry.

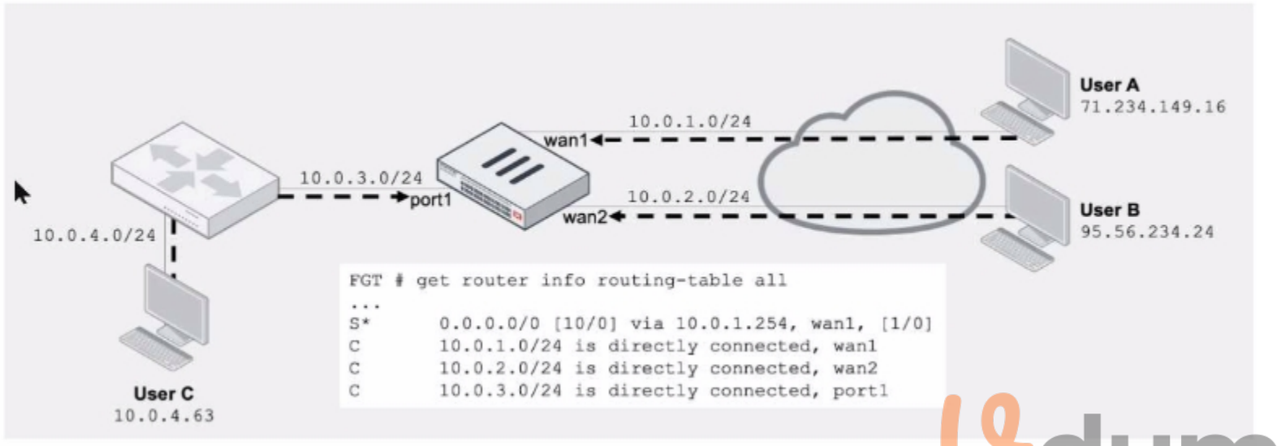
```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81,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

Correct Answer: B, D
Section:

QUESTION 4
Refer to the exhibit.



Assuming a default configuration, which three statements are true? (Choose three)

A. Strict RPF is enabled by default.
B. User B: Fail. There is no route to 95.56.234.24 using wan2 in the routing table.
C. User A: Pass. The default static route through wan1 passes the RPF check regardless of the source IP address.
D. User B: Pass. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
E. User C: Fail. There is no route to 10.0.4.63 using port1 in the touting table.

Correct Answer: B, D, E
Section:

QUESTION 5
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.

Correct Answer: C, D
Section:

QUESTION 6

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'

Correct Answer: D
Section:

QUESTION 7
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.

Correct Answer: B, C
Section:

QUESTION 8
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.

Correct Answer: B, D
Section:

QUESTION 9
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.

Correct Answer: D
Section:

QUESTION 10
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.

Correct Answer: C
Section:

QUESTION 11
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 _ENCI none
ike 0: Remotesite:3:              type=OAKLEY HASH RYPT _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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000C5C64D5CBA90B873F150CB8B5CCZA
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.

Correct Answer: C, D
Section:

QUESTION 12
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.

Correct Answer: B
Section:

QUESTION 13
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

Correct Answer: A
Section:

QUESTION 14
Exhibit.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-iD6 ::
    set proxv-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username
    set ddns-server-ip 0.0.0.0
    set dons-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.
An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however the web filter is not inspecting any traffic that is passing through the policy.
What must the administrator do to fix the issue?

A. Disable webfilter-force-off.
B. Increase webfilter-timeout.
C. Enable fortiguard-anycast.
D. Change protocol to TCP.

Correct Answer: A
Section:

QUESTION 15
Which statement about IKEv2 is true?

A. Both IKEv1 and IKEv2 share the feature of asymmetric authentication.
B. IKEv1 and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.
C. IKEv1 and IKEv2 use same TCP port but run on different UDP ports.
D. IKEv1 and IKEv2 share the concept of phase1 and phase2.

Correct Answer: B
Section:

QUESTION 16
Exhibit 1.

```
config system global
   set snat-route-change disable
end
-----------------
config router static
   edit 1
      set gateway 10.200.1.254
      set priority 5
      set device "port1"
   next
   edit 2
      set gateway 10.200.2.254
      set priority 10
      set device "port2"
   next
end
```

Exhibit 2.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.
An administrator would like to lest session failover between the two service provider connections.
Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two)

A. Change the priority of the port! static route to 11.

B. Change the priority of the port2 static route to 5.
C. Configure unset snat-route-change to return it to the default setting.
D. Configure set snat-route-change enable.

Correct Answer: A, D
Section:

QUESTION 17
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.

Correct Answer: A, D
Section:

QUESTION 18
Refer to the exhibit.

```
# diagnose sys top
Run Time:  0 days, 0 hours and 18 minutes
0U, 0N, 1S, 95I, 0WA, 0HI, 0SI, 0ST; 16063, 12523F
        pyfcgid      248      S       2.9     3.8  9
         newcli      251      R       0.1     1.0  5
  merged_daemons     185      S       0.1     0.7  6
        miglogd      177      S       0.0     6.8  0
        pyfcgid      249      S       0.0     3.0  2
        pyfcgid      246      S       0.0     2.8  5
        reportd      197      S       0.0     2.7  2
        cmdbsvr      113      S       0.0     2.4  7
```

Which three pieces of information does the diagnose sys top command provide? (Choose three)

A. The miglogd daemon is running on CPU core ID 0.
B. The diagnose sys top command has been running for 18 minutes.
C. The miglogd daemon would be on top of the list, if the administrator pressed m on the keyboard.

D. The cmdbsvr process is occupying 2.4% of the total user memory space.
E. If the neweli daemon continues to be in the R state, it will need to be manually restarted.

Correct Answer: A, B, D
Section:

QUESTION 19
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
tus 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>
.2.2.1/32        100.64.2.1                          32768        0 ? <-/1>
.8.8.8/32        100.64.2.254    0              100      0        0 ? <-/1>
0.20.30.0/24     172.16.54.115   0              100      0        0 i <-/1>


l 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.

Correct Answer: A, D
Section:

QUESTION 20
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

Correct Answer: A, C
Section:

QUESTION 21
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

Correct Answer: A, C
Section:

QUESTION 22
Which exchange lakes care of DoS protection in IKEv2?

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

Correct Answer: C
Section: