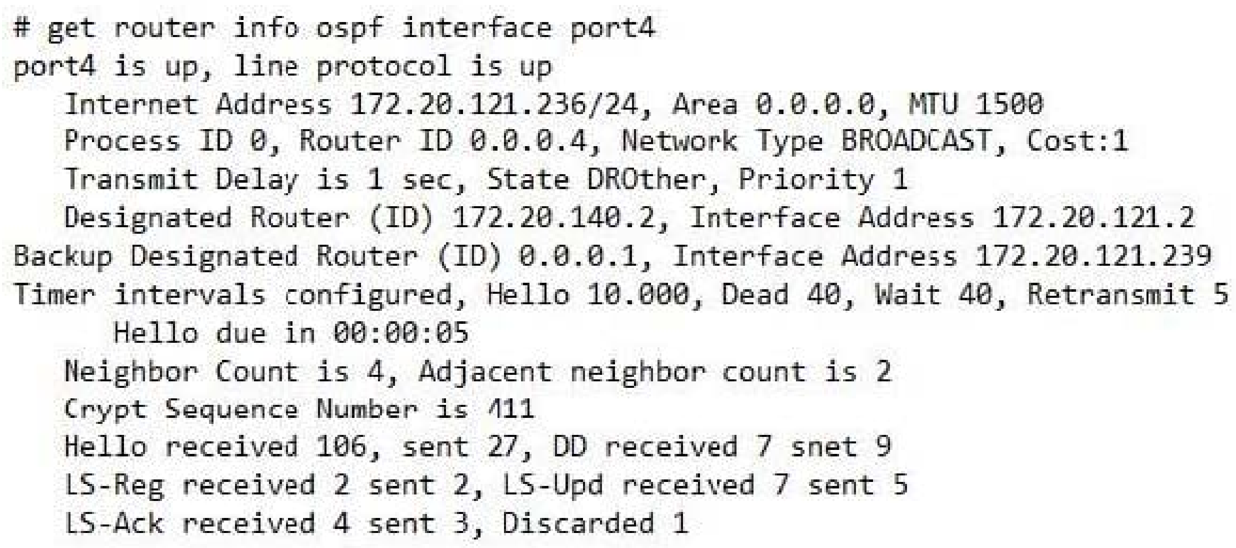
NSE7_EFW Q&As

NSE7 Enterprise Firewall - FortiOS 5.4

QUESTION 1

View the exhibit, which contains the output of a debug command, and then answer the question below.



```
# 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, 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 7 snet 9
   LS-Reg received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

Which of the following statements about the exhibit are true? (Choose two.)

A. In the network on port4, two OSPF routers are down.

B. Port4 is connected to the OSPF backbone area.

C. The local FortiGate\\'s OSPF router ID is 0.0.0.4

D. The local FortiGate has been elected as the OSPF backup designated router.

Correct Answer: BC

QUESTION 2

Examine the following partial outputs from two routing debug commands; then answer the question below.

# get router info kernel

tab=254 vf=0 scope=0type=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=10.200.1.254 dev=2(port1)

tab=254 vf=0 scope=0type=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=10.200.2.254 dev=3(port2)

tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254

gwy=0.0.0.0 dev=4(port3)

get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, portl [10/0] via 10.200.2.254, port2,

[10/0] dO.0.1.0/24 is directly connected, port3 dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is

directly connected, port2 Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!

B. port2.

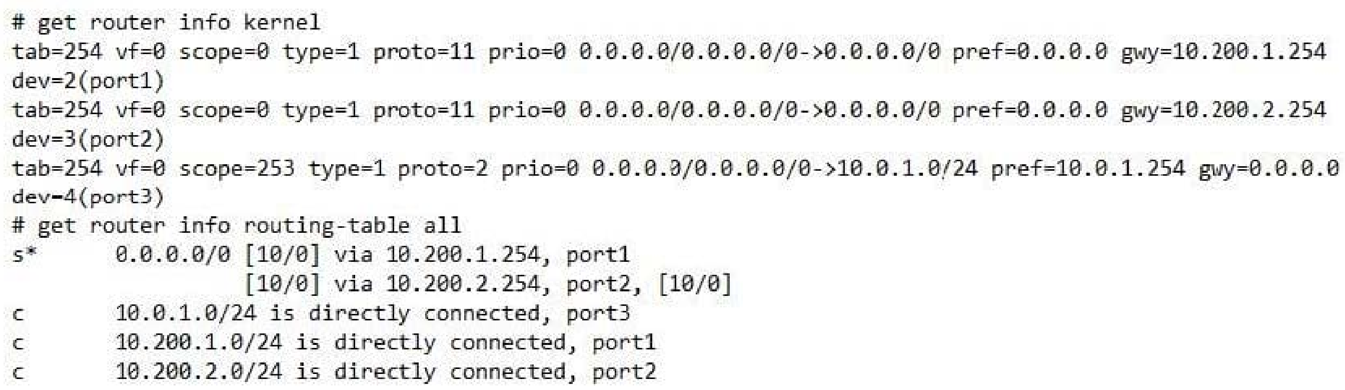
C. Both portl and port2.

D. port3.

Correct Answer: B

QUESTION 3

View these partial outputs from two routing debug commands:



```
# 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=10.200.1.254
dev=2(port1)
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=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev-4(port3)
# get router info routing-table all
s*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                  [10/0] via 10.200.2.254, port2, [10/0]
c       10.0.1.0/24 is directly connected, port3
c       10.200.1.0/24 is directly connected, port1
c       10.200.2.0/24 is directly connected, port2
```

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

A. Both port1 and port2

B. port3

C. port1

D. port2

Correct Answer: C

QUESTION 4

Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

A. Primary unit stops sending HA heartbeat keepalives.

B. The FortiGuard license for the primary unit is updated.

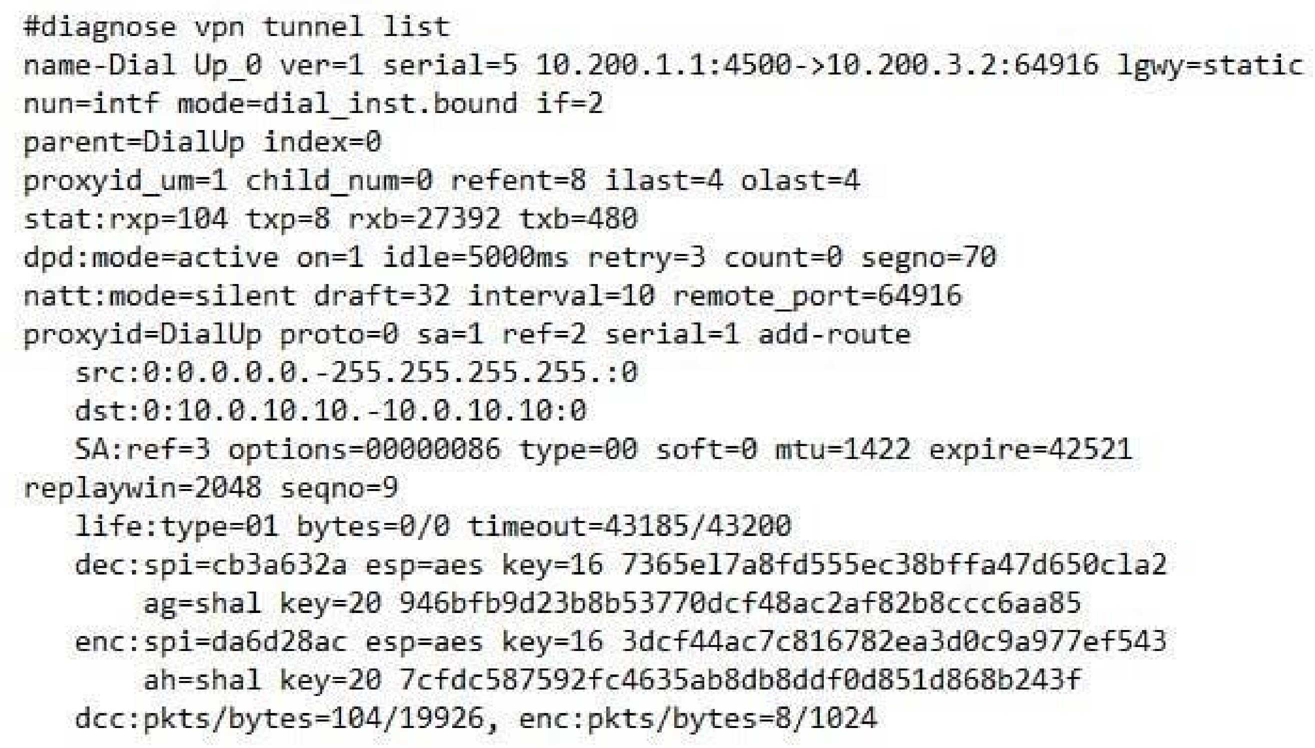
C. One of the monitored interfaces in the primary unit is disconnected.

D. A secondary unit is removed from the HA cluster.

Correct Answer: AB

QUESTION 5

Examine the output from the `diagnose vpn tunnel list\\' command shown in the exhibit; then answer the question below.



```
#diagnose vpn tunnel list
name-Dial Up_0 ver=1 serial=5 10.200.1.1:4500->10.200.3.2:64916 lgwy=static
nun=intf mode=dial_inst.bound if=2
parent=DialUp index=0
proxyid_um=1 child_num=0 refent=8 ilast=4 olast=4
stat:rxp=104 txp=8 rxb=27392 txb=480
dpd:mode=active on=1 idle=5000ms retry=3 count=0 segno=70
natt:mode=silent draft=32 interval=10 remote_port=64916
proxyid=DialUp proto=0 sa=1 ref=2 serial=1 add-route
   src:0:0.0.0.0.-255.255.255.255.:0
   dst:0:10.0.10.10.-10.0.10.10:0
   SA:ref=3 options=00000086 type=00 soft=0 mtu=1422 expire=42521
replaywin=2048 seqno=9
   life:type=01 bytes=0/0 timeout=43185/43200
   dec:spi=cb3a632a esp=aes key=16 7365el7a8fd555ec38bffa47d650cla2
       ag=shal key=20 946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
   enc:spi=da6d28ac esp=aes key=16 3dcf44ac7c816782ea3d0c9a977ef543
       ah=shal key=20 7cfdc587592fc4635ab8db8ddf0d851d868b243f
   dcc:pkts/bytes=104/19926, enc:pkts/bytes=8/1024
```

Which command can be used to sniffer the ESP traffic for the VPN DialUP_0?

A. diagnose sniffer packet any `port 500\\'

B. diagnose sniffer packet any `esp\\'

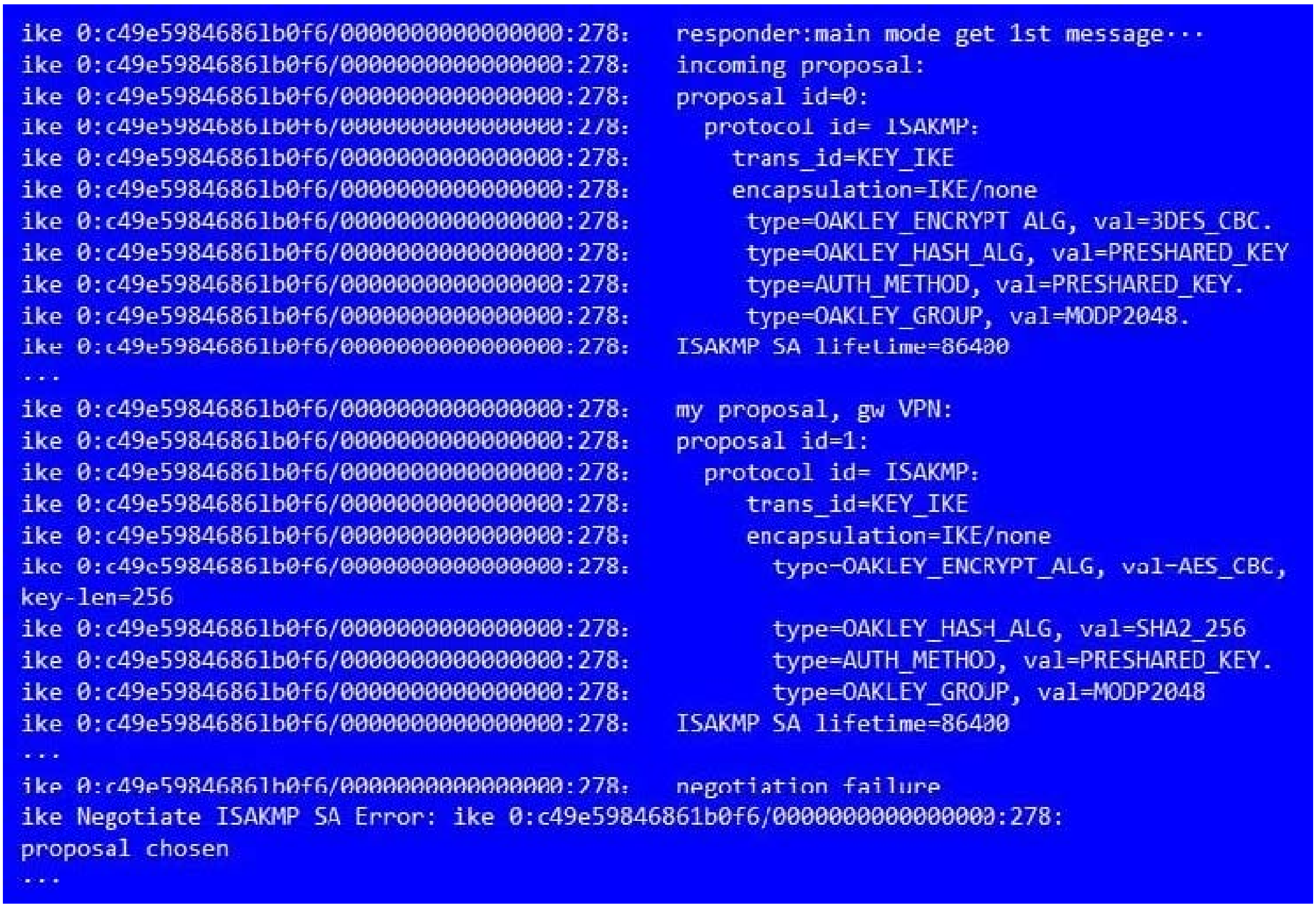
C. diagnose sniffer packet any `host 10.0.10.10\\'

D. diagnose sniffer packet any `port 4500\\'

Correct Answer: B

QUESTION 6

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.



```
ike 0:c49e59846861b0f6/0000000000000000:278:   responder:main mode get 1st message···
ike 0:c49e59846861b0f6/0000000000000000:278:   incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278:   proposal id=0:
ike 0:c49e59846861b0f6/0000000000000000:278:     protocol id= ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:       trans_id=KEY_IKE
ike 0:c49e59846861b0f6/0000000000000000:278:       encapsulation=IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:        type=OAKLEY_ENCRYPT ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:        type=OAKLEY_HASH_ALG, val=PRESHARED_KEY
ike 0:c49e59846861b0f6/0000000000000000:278:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:        type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278:   ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278:   my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278:   proposal id=1:
ike 0:c49e59846861b0f6/0000000000000000:278:     protocol id= ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:        trans_id=KEY_IKE
ike 0:c49e59846861b0f6/0000000000000000:278:        encapsulation=IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_HASH_ALG, val=SHA2_256
ike 0:c49e59846861b0f6/0000000000000000:278:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:          type=OAKLEY_GROUP, val=MODP2048
ike 0:c49e59846861b0f6/0000000000000000:278:   ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278:   negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn\\'t the tunnel come up?

A. The pre-shared keys do not match.

B. The remote gateway\\'s phase 2 configuration does not match the local gateway\\'s phase 2 configuration.

C. The remote gateway\\'s phase 1 configuration does not match the local gateway\\'s phase 1 configuration.

D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Correct Answer: C

QUESTION 7

In which of the following states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting to complete the three-way handshake.

B. A TCP session waiting for FIN ACK.

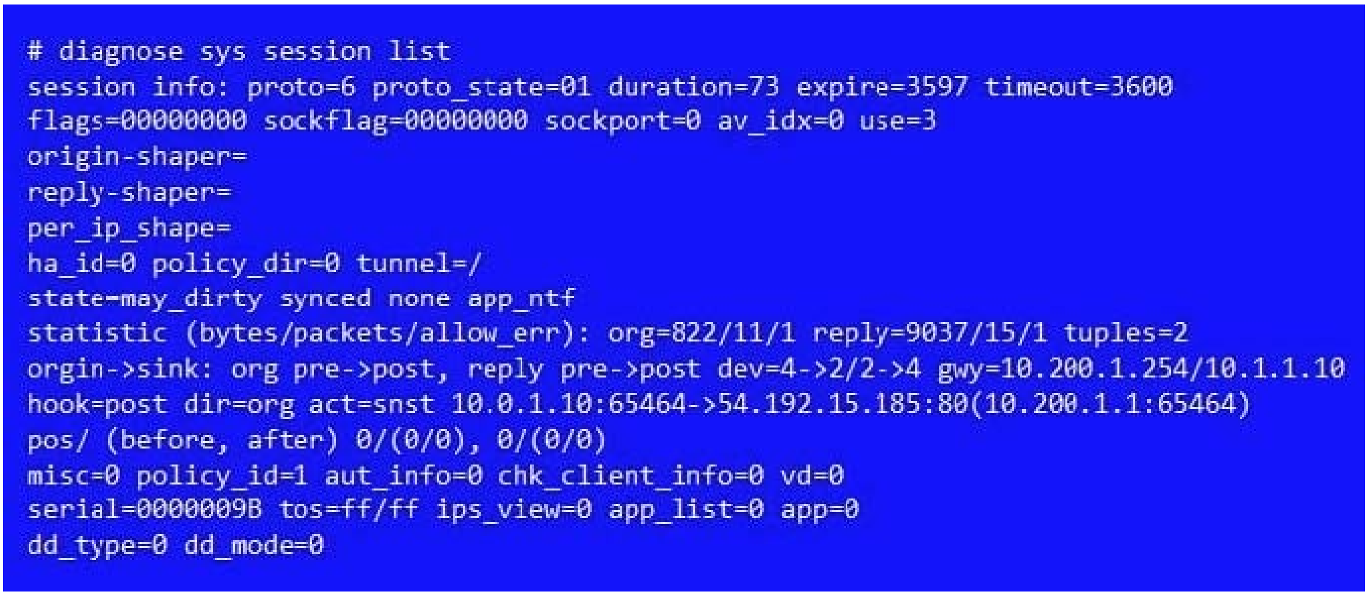
C. A UDP session with packets sent and received.

D. A UDP session with only one packet received.

Correct Answer: BC

QUESTION 8

View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.



```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shape=
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.1.1.10
hook=post dir=org act=snst 10.0.1.10:65464->54.192.15.185:80(10.200.1.1:65464)
pos/ (before, after) 0/(0/0), 0/(0/0)
misc=0 policy_id=1 aut_info=0 chk_client_info=0 vd=0
serial=0000009B tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement is correct regarding the output?

A. This session is for HA heartbeat traffic.

B. This session is synced with the slave unit.

C. The inspection of this session has been offloaded to the slave unit.

D. This session cannot be synced with the slave unit.

Correct Answer: B

QUESTION 9

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the `diagnose debug authd fsso list\\' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

A. The user student must not be listed in the CA\\'s ignore user list.

B. The user student must belong to one or more of the monitored user groups.

C. The student workstation\\'s IP subnet must be listed in the CA\\'s trusted list.

D. At least one of the student\\'s user groups must be allowed by a FortiGate firewall policy.

Correct Answer: BD

QUESTION 10

What is the purpose of an internal segmentation firewall (ISFW)?

A. It inspects incoming traffic to protect services in the corporate DMZ.

B. It is the first line of defense at the network perimeter.

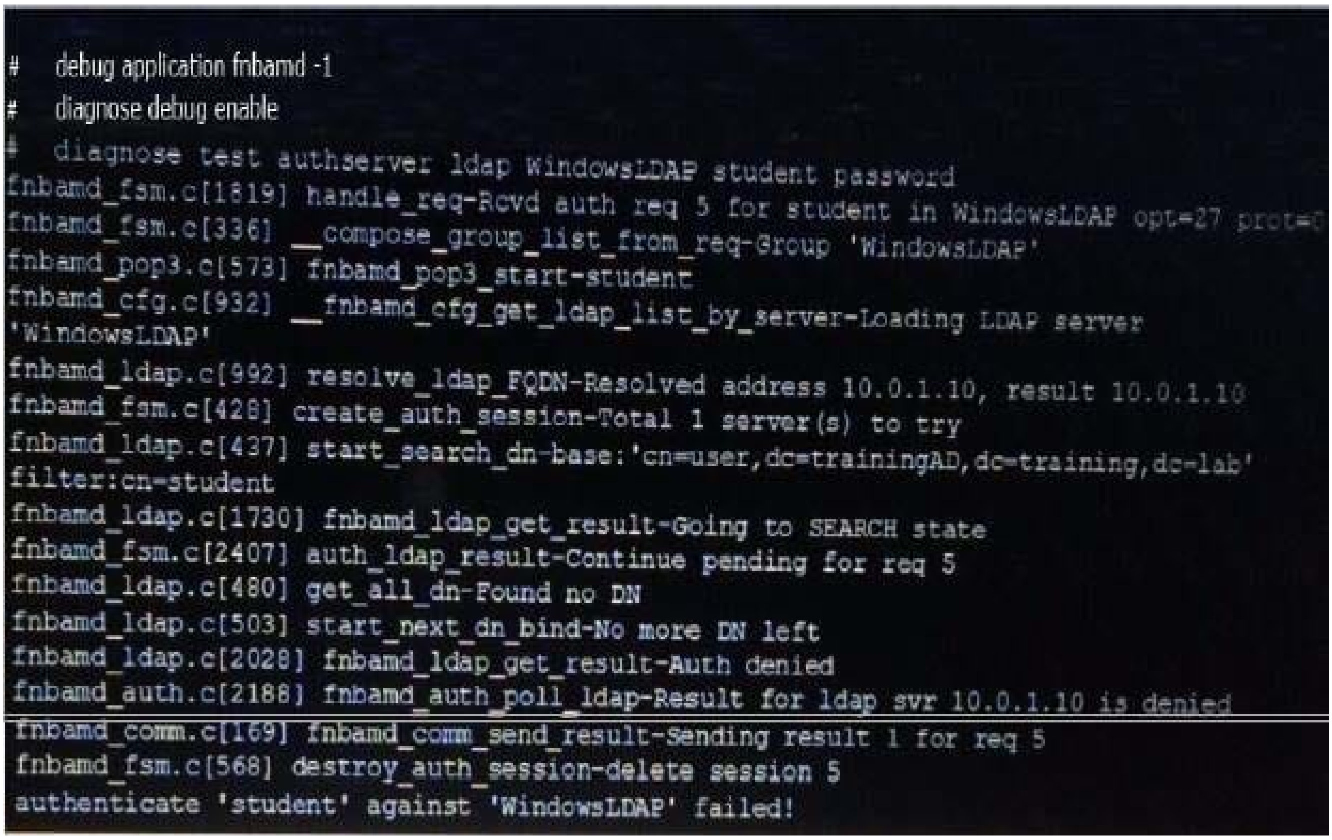
C. It splits the network into multiple security segments to minimize the impact of breaches.

D. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

Correct Answer: B

QUESTION 11

An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.



```
#   debug application fnbamd -1
#   diagnose debug enable
#   diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server(s) to try
fnbamd_ldap.c[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

A. User student is not found in the LDAP server.

B. User student is using a wrong password.

C. The FortiGate has been configured with the wrong password for the LDAP administrator.

D. The FortiGate has been configured with the wrong authentication schema.

Correct Answer: A

QUESTION 12

What conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. IP addresses are in the same subnet.

B. Hello and dead intervals match.

C. OSPF IP MTUs match.

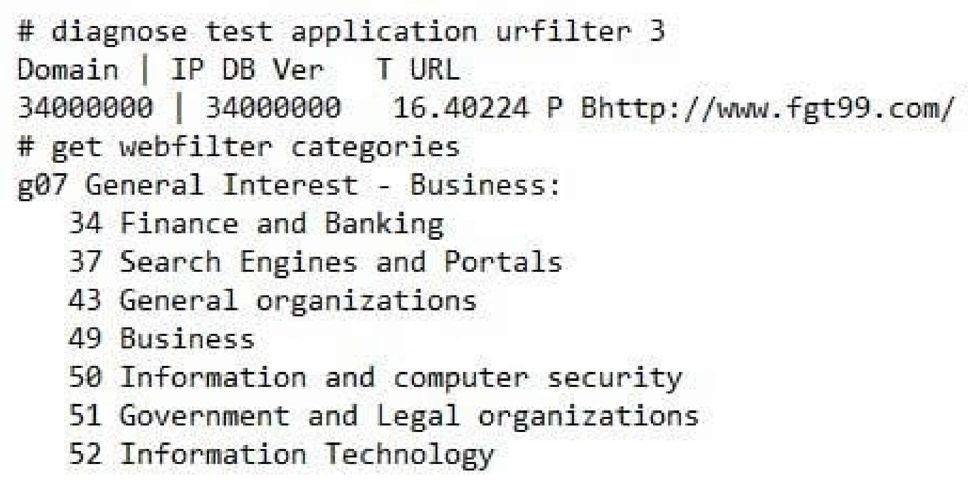
D. OSPF peer IDs match.

E. OSPF costs match.

Correct Answer: ABD

QUESTION 13

Examine the partial output from two web filter debug commands; then answer the question below:



```
# diagnose test application urlfilter 3
Domain | IP DB Ver   T URL
34000000 | 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
    34 Finance and Banking
    37 Search Engines and Portals
    43 General organizations
    49 Business
    50 Information and computer security
    51 Government and Legal organizations
    52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking

B. General organization.

C. Business.

D. Information technology.

Correct Answer: C

QUESTION 14

The CLI command set intelligent-mode controls the IPS engine\\'s adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

A. Determines the optimal number of IPS engines required based on system load.

B. Downloads signatures on demand from FDS based on scanning requirements.

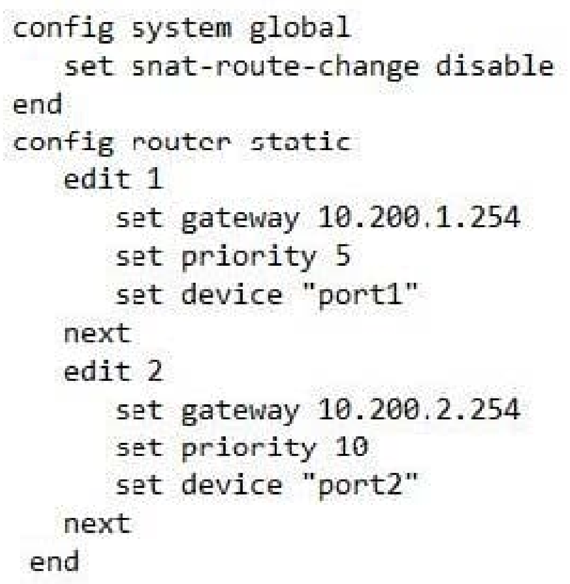
C. Determines when it is secure enough to stop scanning session traffic.

D. Choose a matching algorithm based on available memory and the type of inspection being performed.

Correct Answer: D

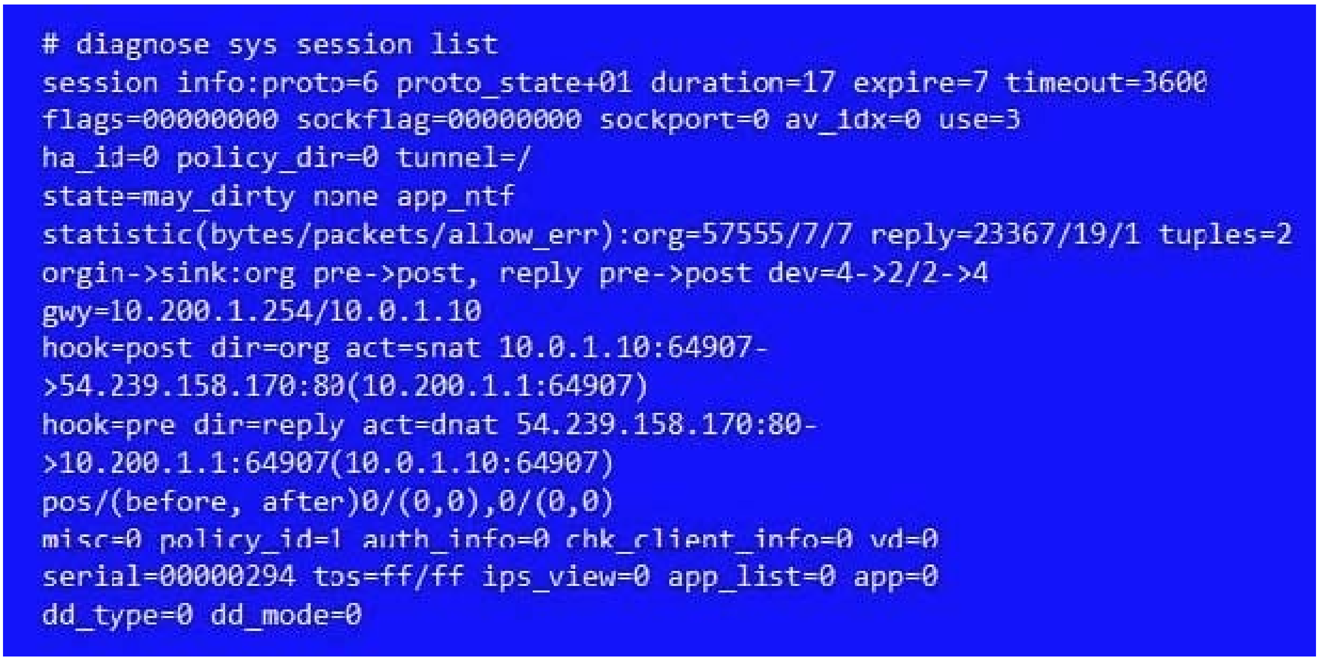
QUESTION 15

View the following FortiGate configuration.



```
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
```

All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network:



```
# diagnose sys session list
session info:proto=6 proto_state+01 duration=17 expire=7 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic(bytes/packets/allow_err):org=57555/7/7 reply=23367/19/1 tuples=2
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)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user\\'s session?

A. The session would remain in the session table, and its traffic would still egress from port1.

B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

C. The session would remain in the session table, and its traffic would start to egress from port2.

D. The session would be deleted, so the client would need to start a new session.

Correct Answer: D

[Latest NSE7_EFW Dumps](https://www.leads4pass.com/nse7_efw.html) [NSE7_EFW VCE Dumps](https://www.leads4pass.com/nse7_efw.html) [NSE7_EFW Study Guide](https://www.leads4pass.com/nse7_efw.html)