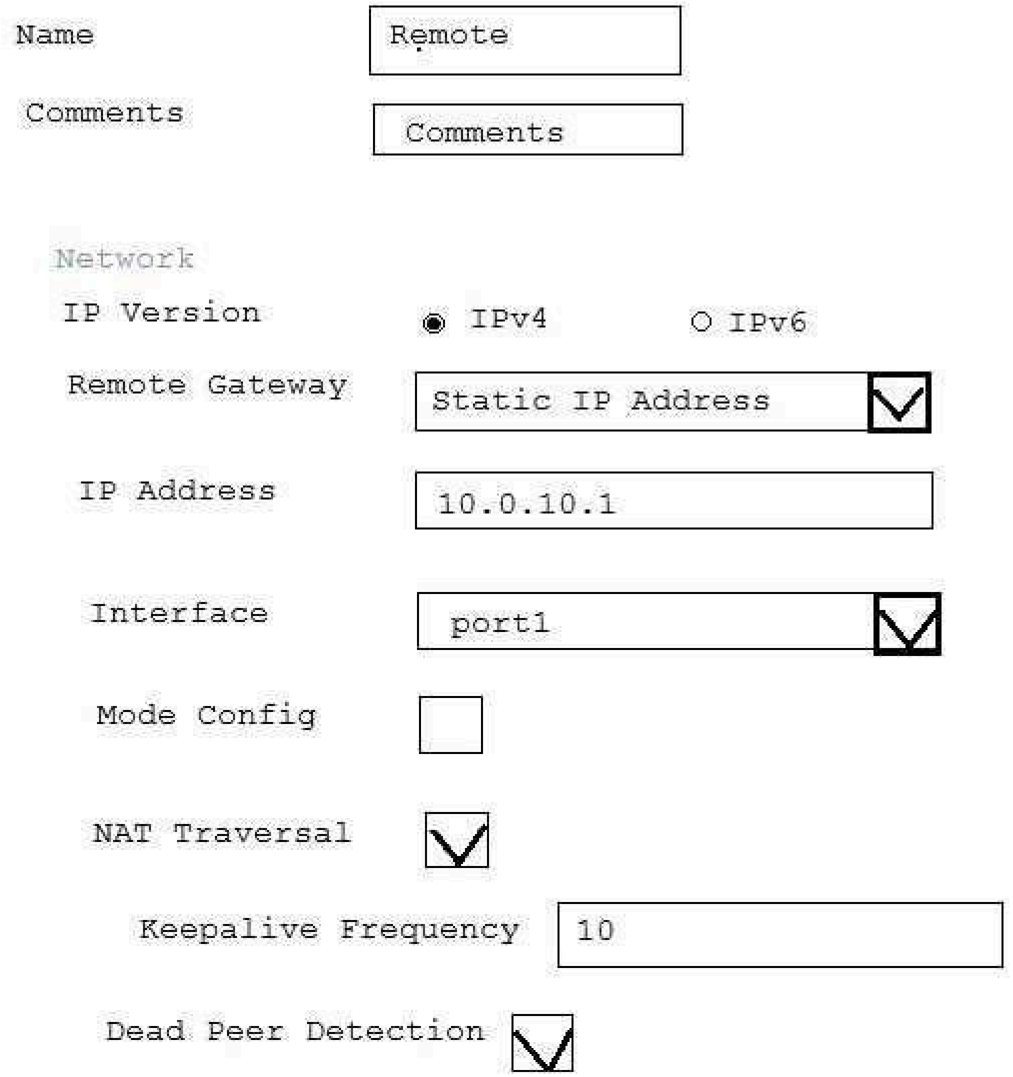
NSE 7 - Enterprise Firewall 7.0

1. Examine the IPsec configuration shown in the exhibit; then answer the question below.



Name	Remote
Comments	Comments

Network

IP Version	● IPv4 ○ IPv6
Remote Gateway	Static IP Address
IP Address	10.0.10.1
Interface	port1
Mode Config	□
NAT Traversal	☑
Keepalive Frequency	10
Dead Peer Detection	☑

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands:

-diagnose vpn ike log-filter src-addr4 10.0.10.1

-diagnose debug application ike -1

-diagnose debug enable

The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn't there any output?

A. The IKE real time shows the phases 1 and 2 negotiations only. It does not show any more output once the tunnel is up.

B. The log-filter setting is set incorrectly. The VPN's traffic does not match this filter.

C. The IKE real time debug shows the phase 1 negotiation only. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.

D. The IKE real time debug shows error messages only. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer(s): B

---

2. Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

□ A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.

□ B. SIP ALG supports SIP HA failover; SIP helper does not.

□ C. SIP ALG supports SIP over IPv6; SIP helper does not.

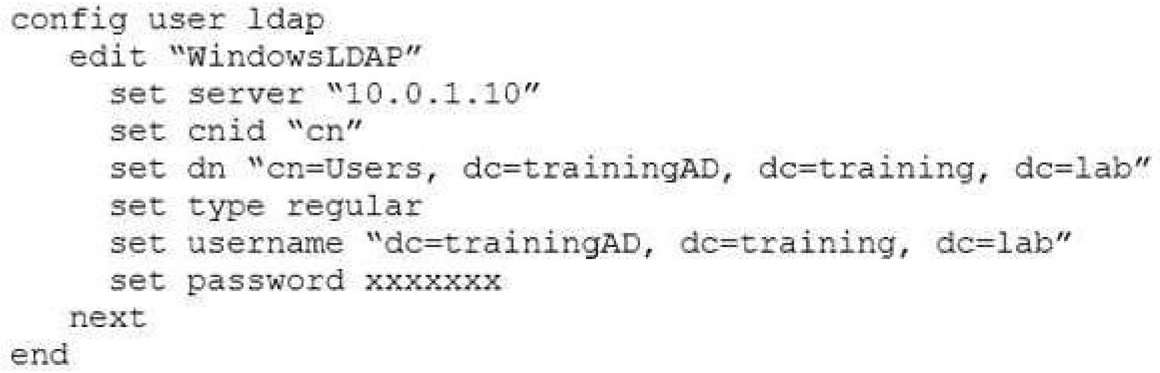
□ D. SIP ALG can create expected sessions for media traffic; SIP helper does not.

□ E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Answer(s): B C D

---

3. A FortiGate device has the following LDAP configuration:



```
config user ldap
   edit "WindowsLDAP"
     set server "10.0.1.10"
     set cnid "cn"
     set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "dc=trainingAD, dc=training, dc=lab"
     set password xxxxxxx
   next
end
```

The administrator executed the ‘dsquery’ command in the Windows LDAp server 10.0.1.10, and got the following output:

>dsquery user –samid administrator

“CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab”

Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.

B. username.

C. password.

D. dn.

Answer(s): B

---

4. 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.

Answer(s): A D

---

5. An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.

B. TCP half close.

C. TCP time wait.

D. TCP session time to live.

Answer(s): A

---

6. An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2
What information is included in the output of the sniffer? (Choose two.)

□ A. Ethernet headers.

□ B. IP payload.

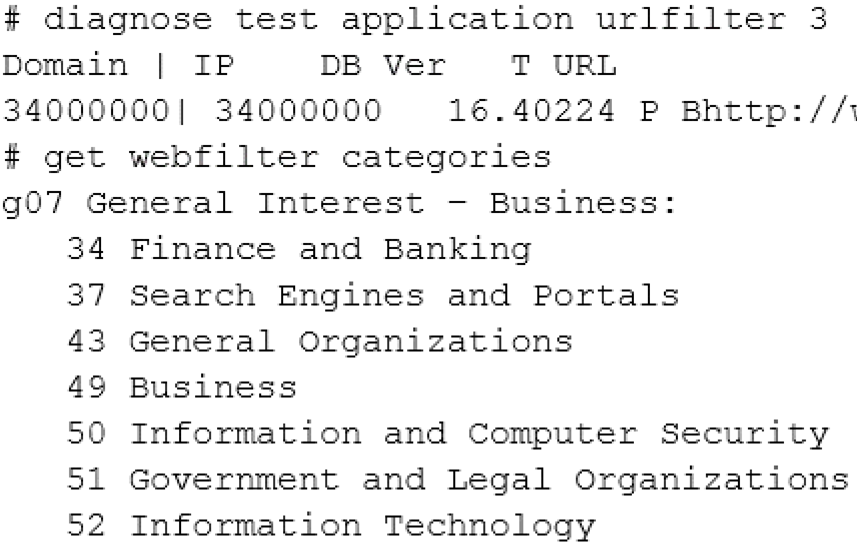
□ C. IP headers.

□ D. Port names.

Answer(s): B C

---

7. 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.

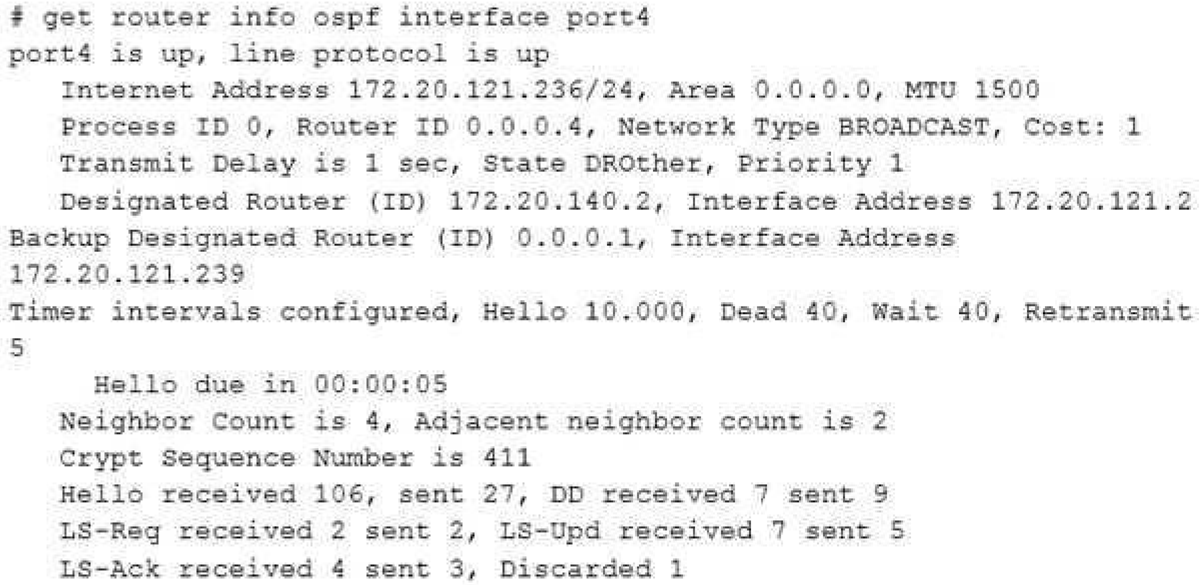
C. Business.

D. Information technology.

Answer(s): C

---

8. Examine the output of the ‘get router info ospf interface’ command shown in the exhibit; 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 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

Which statements are true regarding the above output? (Choose two.)

□ A. The port4 interface is connected to the OSPF backbone area.

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

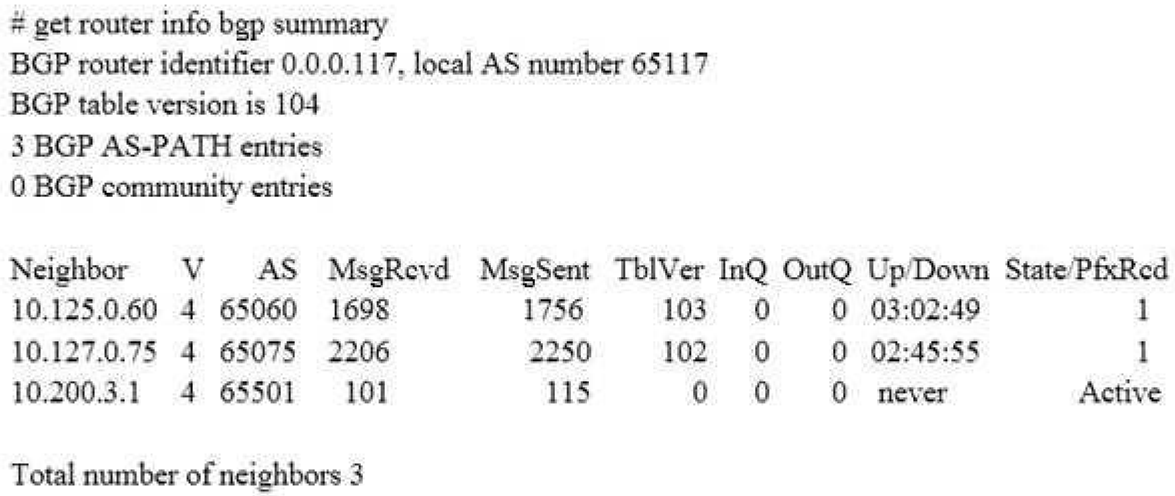
□ C. There are at least 5 OSPF routers connected to the port4 network.

□ D. Two OSPF routers are down in the port4 network.

Answer(s): A C

---

9. Examine the output of the ‘get router info bgp summary’ command shown in the exhibit; then answer the question below.



```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor     V    AS    MsgRcvd   MsgSent  TblVer  InQ  OutQ  Up/Down   State/PfxRcd
10.125.0.60  4  65060   1698       1756     103     0     0   03:02:49            1
10.127.0.75  4  65075   2206       2250     102     0     0   02:45:55            1
10.200.3.1   4  65501    101        115       0     0     0    never          Active

Total number of neighbors 3
```

Which statements are true regarding the output in the exhibit? (Choose two.)

□ A. BGP state of the peer 10.125.0.60 is Established.

□ B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.

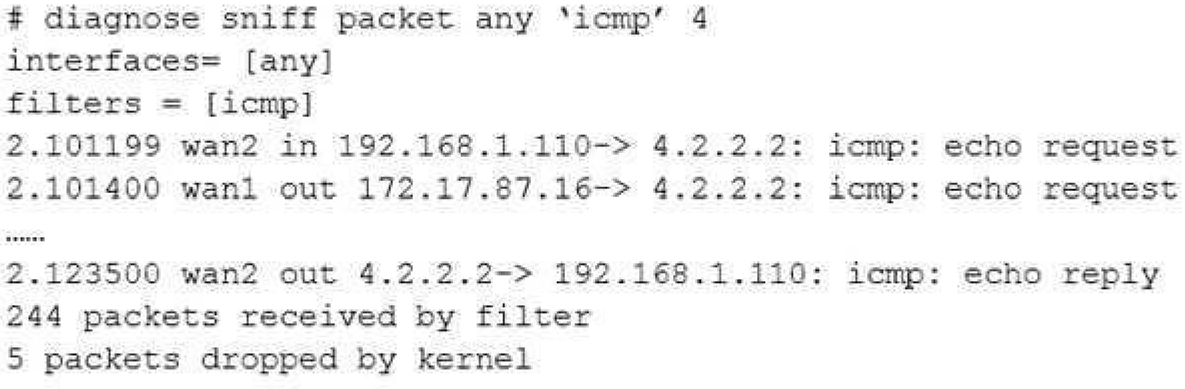
□ C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.

□ D. The local BGP peer has received a total of 3 BGP prefixes.

Answer(s): A C

---

10. Examine the following partial output from a sniffer command; then answer the question below.



```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
......
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn’t match the sniffer filter.

B. Number of total packets dropped by the FortiGate.

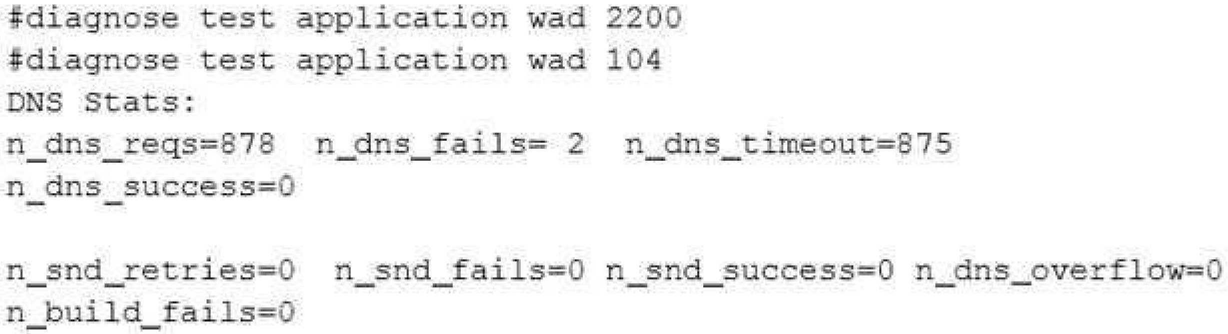
C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.

D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Answer(s): D

---

11. A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-dns-timeout counter is increasing:



```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878  n_dns_fails= 2  n_dns_timeout=875
n_dns_success=0

n_snd_retries=0  n_snd_fails=0 n_snd_success=0 n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

A. The connectivity between the FortiGate unit and the DNS server.

B. The connectivity between the client workstations and the DNS server.

C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.

D. That DNS service is enabled in the explicit web proxy interface.

Answer(s): A

---

12. Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

A. Diagnose debug application radius -1.

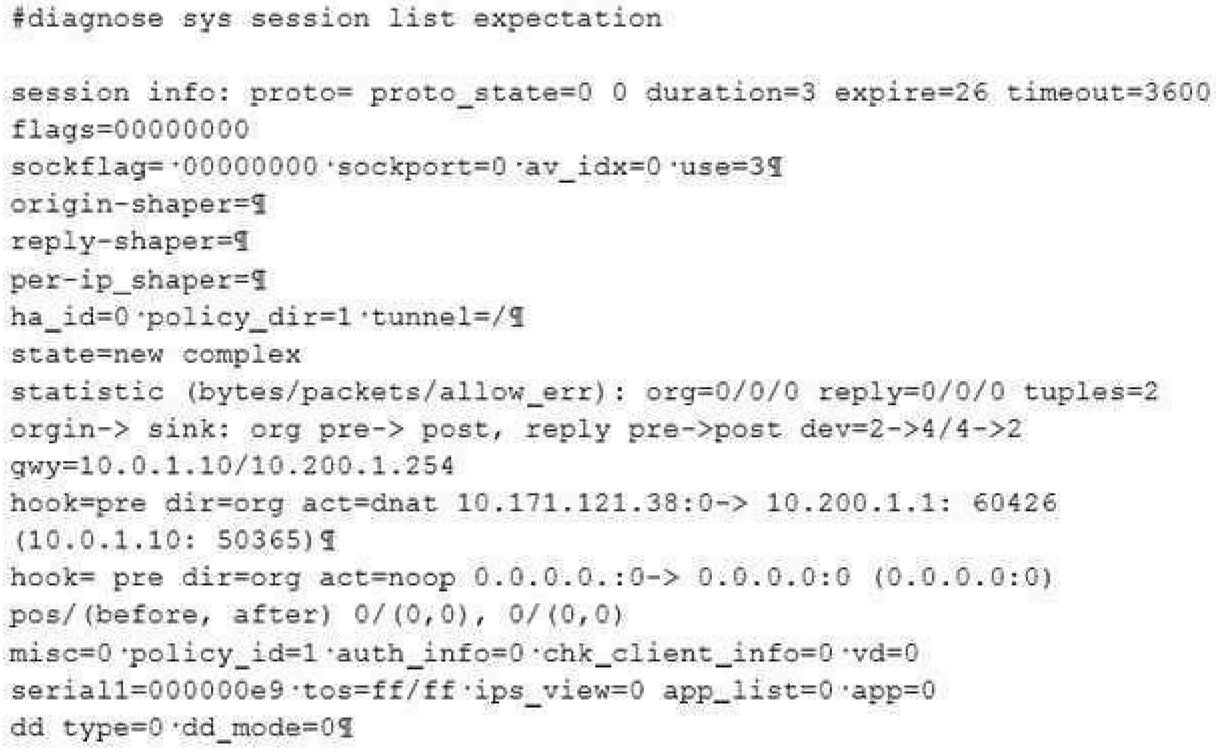
B. Diagnose debug application fnbamd -1.

C. Diagnose authd console –log enable.

D. Diagnose radius console –log enable.

Answer(s): B

13. Examine the output of the ‘diagnose sys session list expectation’ command shown in the exhibit; than answer the question below.



```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
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 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=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)¶
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=1·auth_info=0·chk_client_info=0·vd=0
serial1=000000e9·tos=ff/ff·ips_view=0 app_list=0·app=0
dd type=0·dd_mode=0¶
```

Which statement is true regarding the session in the exhibit?

A. It was created by the FortiGate kernel to allow push updates from FotiGuard.

B. It is for management traffic terminating at the FortiGate.

C. It is for traffic originated from the FortiGate.

D. It was created by a session helper or ALG.

Answer(s): D

14. An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

☐ A. Router ID.

☐ B. OSPF interface area.

□ C. OSPF interface cost.

□ D. OSPF interface MTU.

□ E. Interface subnet mask.

Answer(s): B D E

---

15. An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug:
-diagnose debug application ike-1
-diagnose debug enable
In which order is each step and phase displayed in the debug output each time a new dial-up user is connecting to the VPN?

A. Phase1; IKE mode configuration; XAuth; phase 2.

B. Phase1; XAuth; IKE mode configuration; phase2.

C. Phase1; XAuth; phase 2; IKE mode configuration.

D. Phase1; IKE mode configuration; phase 2; XAuth.

Answer(s): B

---

16. Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

A. Group ID.

B. Group name.

C. Session pickup.

D. Gratuitous ARPs.

Answer(s): A

---

17. When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.

B. The server requires more information from the user, such as the token code for two-factor authentication.

C. The user credentials are wrong.

D. The user account is not found in the server.

Answer(s): B

---

18. The logs in a FSSO collector agent (CA) are showing the following error:
failed to connect to registry: PIKA1026 (192.168.12.232)
What can be the reason for this error?

A. The CA cannot resolve the name of the workstation.

B. The FortiGate cannot resolve the name of the workstation.

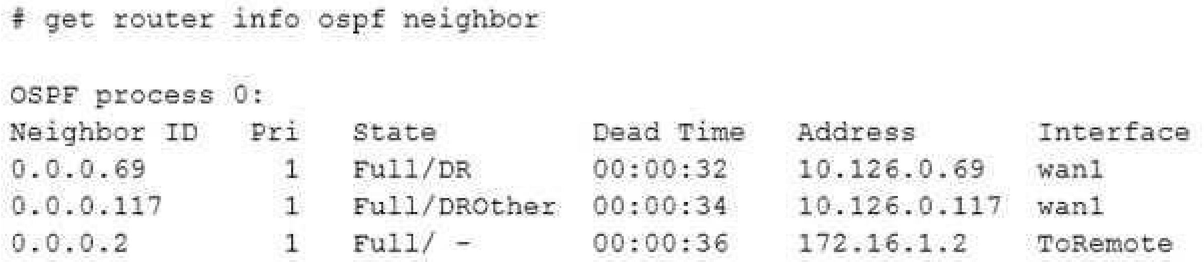
C. The remote registry service is not running in the workstation 192.168.12.232.

D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer(s): C

---

19. Examine the output of the ‘get router info ospf neighbor’ command shown in the exhibit; then answer the question below.



```
# get router info ospf neighbor

OSPF process 0:
Neighbor ID    Pri   State          Dead Time   Address        Interface
0.0.0.69         1   Full/DR        00:00:32    10.126.0.69    wan1
0.0.0.117        1   Full/DROther   00:00:34    10.126.0.117   wan1
0.0.0.2          1   Full/ -        00:00:36    172.16.1.2     ToRemote
```

Which statements are true regarding the output in the exhibit? (Choose two.) Refer to the exhibit, which shows the output of a debug command.
Which statement about the output is true?

A. TheOSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the war. I network.

B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.

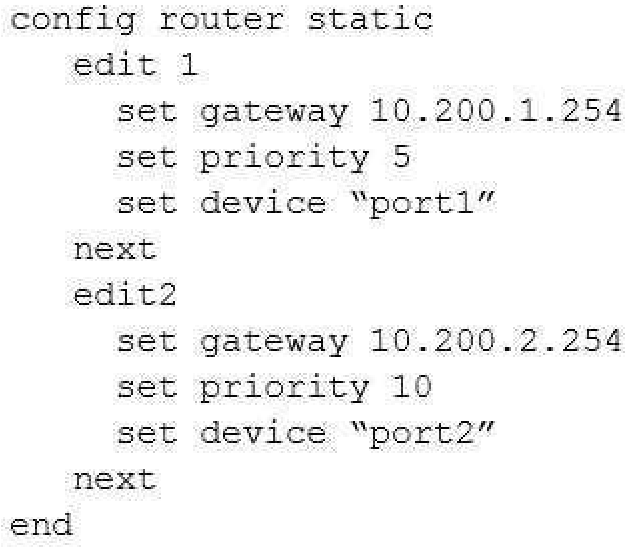
C. The local FortiGate is the designated router for the wan1 network.

D. The interface ToRemote is a point-to-point OSPF network.

Answer(s): D

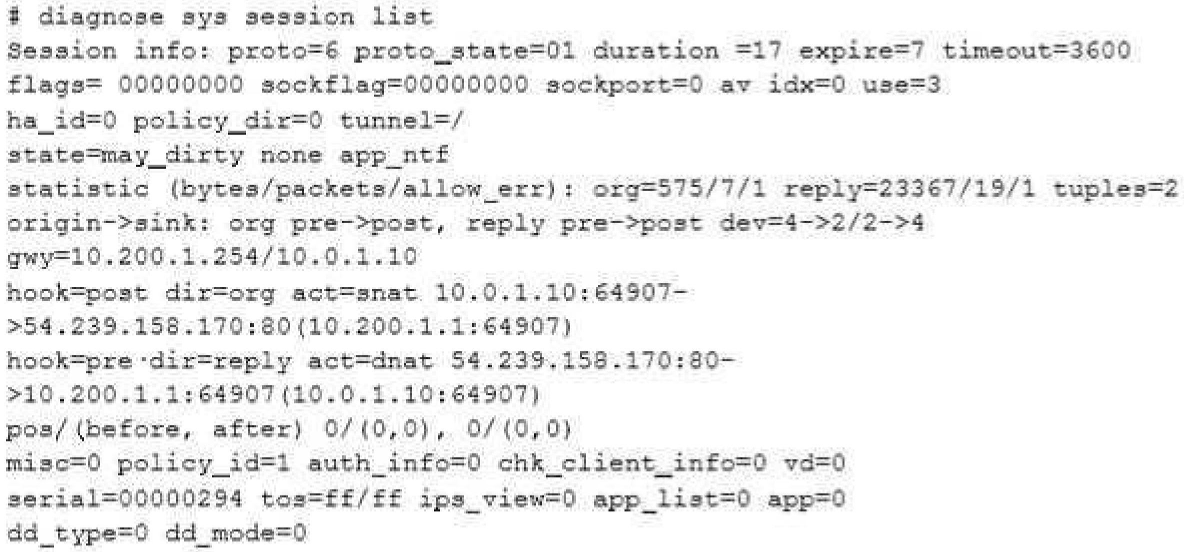
---

20. A FortiGate has two default routes:



```
config router static
   edit 1
      set gateway 10.200.1.254
      set priority 5
      set device "port1"
   next
   edit2
      set gateway 10.200.2.254
      set priority 10
      set device "port2"
   next
end
```

All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:



```
# 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=575/7/1 reply=23367/19/1 tuples=2
origin->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
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. The session would be deleted, and the client would need to start a new session.

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

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

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

Answer(s): D