Exam Questions NSE7

NSE7 Enterprise Firewall - FortiOS 5.4

https://www.2passeasy.com/dumps/NSE7/

NEW QUESTION 1
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V      AS    MsgRcvd   MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
10.200.3.1  4   65501         92       112        0    0     0     never    Connect

Total number of neighbors 1
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
B. The TCP session for the BGP connection to 10.200.3.1 is down.
C. The local peer has received the BGP prefixed from the remote peer.
D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B

NEW QUESTION 2
Examine the output of the 'diagnose ips anomaly list' command shown in the exhibit; then answer the question below.

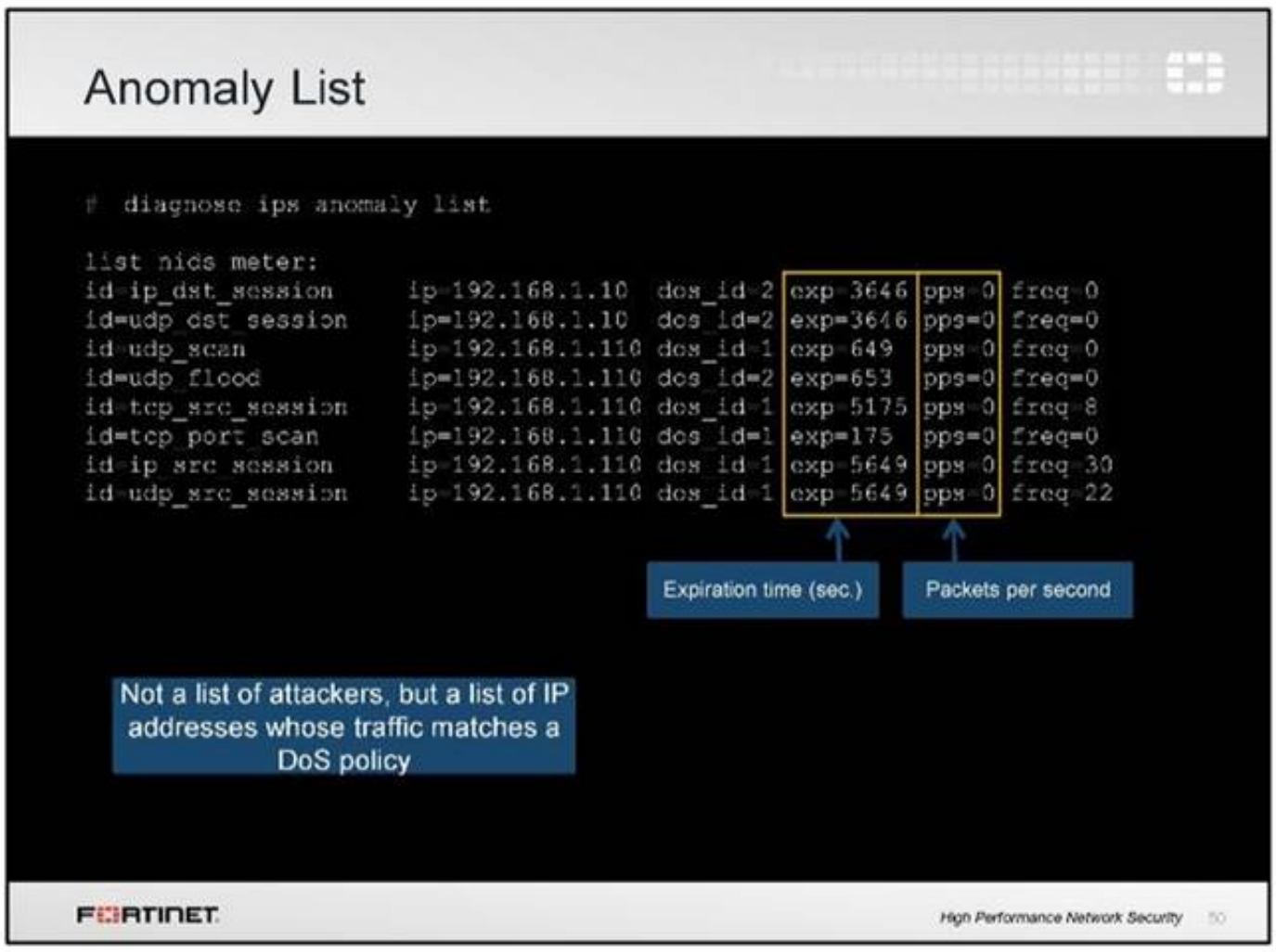
```
# diagnose ips anomaly list

list nids meter:
id=ip_dst_session     ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_dst_session    ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_scan           ip=192.168.1.110   dos_id=1  exp=649   pps=0  freq=0
id=udp_flood          ip=192.168.1.110   dos_id=2  exp=653   pps=0  freq=0
id=tcp_src_session    ip=192.168.1.110   dos_id=1  exp=5175  pps=0  freq=8
id=tcp_port_scan      ip=192.168.1.110   dos_id=1  exp=175   pps=0  freq=0
id=ip_src_session     ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=30
id=udp_src_session    ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=22
```

Which IP addresses are included in the output of this command?

A. Those whose traffic matches a DoS policy.
B. Those whose traffic matches an IPS sensor.
C. Those whose traffic exceeded a threshold of a matching DoS policy.
D. Those whose traffic was detected as an anomaly by an IPS sensor.

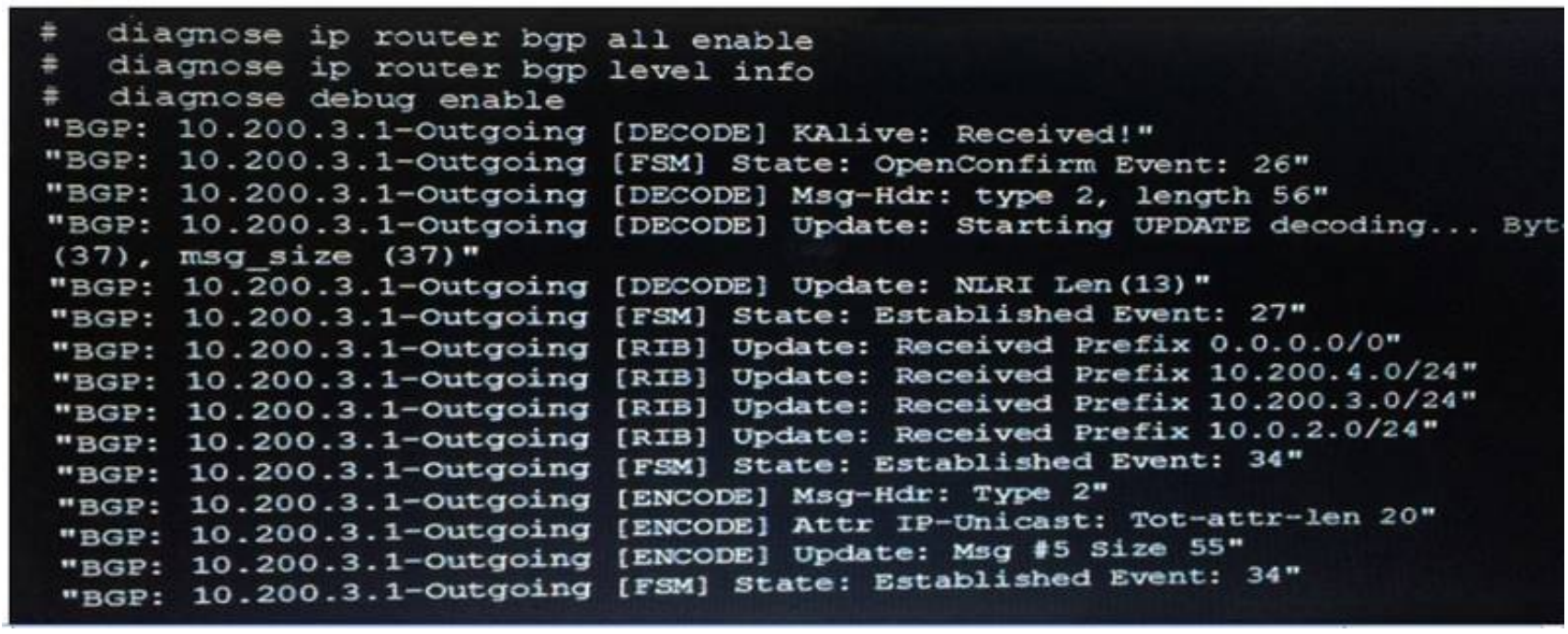
Answer: A

Explanation:



The command '**diagnose ips anomaly list**' lists the statistics for traffic matching any DoS policy. For each IP address and DoS policy, the output displays the expiration time (when the entry will be removed from the DoS table) and the packets per seconds.

NEW QUESTION 3
Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:



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

A. BGP peers have successfully interchanged Open and Keepalive messages.
B. Local BGP peer received a prefix for a default route.
C. The state of the remote BGP peer is OpenConfirm.
D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Answer: AB

NEW QUESTION 4
Which statement is true regarding File description (FD) conserve mode?

A. IPS inspection is affected when FortiGate enters FD conserve mode.
B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
C. FD conserve mode affects all daemons running on the device.
D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 5
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: A

NEW QUESTION 6
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: B

NEW QUESTION 7
Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-miltipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

TheBGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

A. Enable the redistribution of connected routers into BGP.
B. Enable the redistribution of static routers into BGP.
C. Disable the setting network-import-check.

D. Enable the setting ebgp-multipath.

Answer: C

NEW QUESTION 8
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: AB

NEW QUESTION 9
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: C

NEW QUESTION 10
View the exhibit, which contains the partial output of a diagnose command, and then answer the question below.

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.2.0/255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
     ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
  ah=sha1 key20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which of the following statements is correct?

A. Anti-reply is enabled.
B. DPD is disabled.
C. Quick mode selectors are disabled.
D. Remote gateway IP is 10.200.5.1.

Answer: A

NEW QUESTION 10
Examine the following partial outputs from two routing debug commands; then answer the question below:

```
#get router info routing-table database
S      0.0.0.0/. [20/0] via 10.200.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
S*     0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

Why the default route using port2 is not displayed in the output of the second command?

A. It has a lower priority than the default route using port1.
B. It has a higher priority than the default route using port1.
C. It has a higher distance than the default route using port1.
D. It is disabled in the FortiGate configuration.

Answer: A

NEW QUESTION 13
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=57555/7/1 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.

Answer: D

NEW QUESTION 14
View the central management configuration shown in the exhibit, and then answer the question below.

```
config system central-management
   set type fortimanager
   set fmg "10.0.1.242"
   config server-list
      edit 1
         set server-type rating
         set server-address 10.0.1.240
      next
      edit 2
         set server-type update
         set server-address 10.0.1.243
      next
      edit 3
         set server-type rating
         set server-address 10.0.1.244
      next
   end
   set include-default-servers enable
end
```

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

A. 10.0.1.240
B. One of the public FortiGuard distribution servers
C. 10.0.1.244
D. 10.0.1.242

Answer: B

NEW QUESTION 15
View the global IPS configuration, and then answer the question below.

```
config ips global
   set fail-open disable
   set intelligent-mode disable
   set engine-count 0
   set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

A. IPS will scan every byte in every session.
B. FortiGate will spawn IPS engine instances based on the system load.
C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.
D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Answer: A

NEW QUESTION 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.)

A. The interface ToRemote is OSPF network type point-to-point.
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 backup designated router for the wan1 network.
D. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.

Answer: AC

NEW QUESTION 24
View the exhibit, which contains the output of a real-time debug, and then answer the question below.

```
# diagnose debug application urlfilter -1
# diagnose debug enable

msg="received a request /tmp/.ipsengine_498_0_0.url.socket, addr_len=37:
d=www.fortinet.com:80
id=83, vfname='root', vfid=0, profile='default', type=0, client=10.0.1.10,
url_source=1, url="/"
msg="Found it in cache.   URL cat=52" IP cat=52user="N/A" src=10.0.1.10
sport=60348 dst=66.171.121.44 dport=80 service="http" hostname="
www.fortinet.com" url="/" matchType=prefix
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=60348
dst=66.171.121.44
dport=80 service="http" cat=52 cat desc="Information Technology"
hostname="fortinet.com"
url="/"
```

Which of the following statements is true regarding this output? (Choose two.)

A. This web request was inspected using the root web filter profile.
B. FortiGate found the requested URL in its local cache.
C. The requested URL belongs to category ID 52.
D. The web request was allowed by FortiGate.

Answer: BC

NEW QUESTION 26
Which of the following statements are true about FortiManager when it is deployed as a local FDS? (Choose two.)

A. Caches available firmware updates for unmanaged devices.
B. Can be configured as an update server, or a rating server, but not both.
C. Supports rating requests from both managed and unmanaged devices.
D. Provides VM license validation services.

Answer: AD

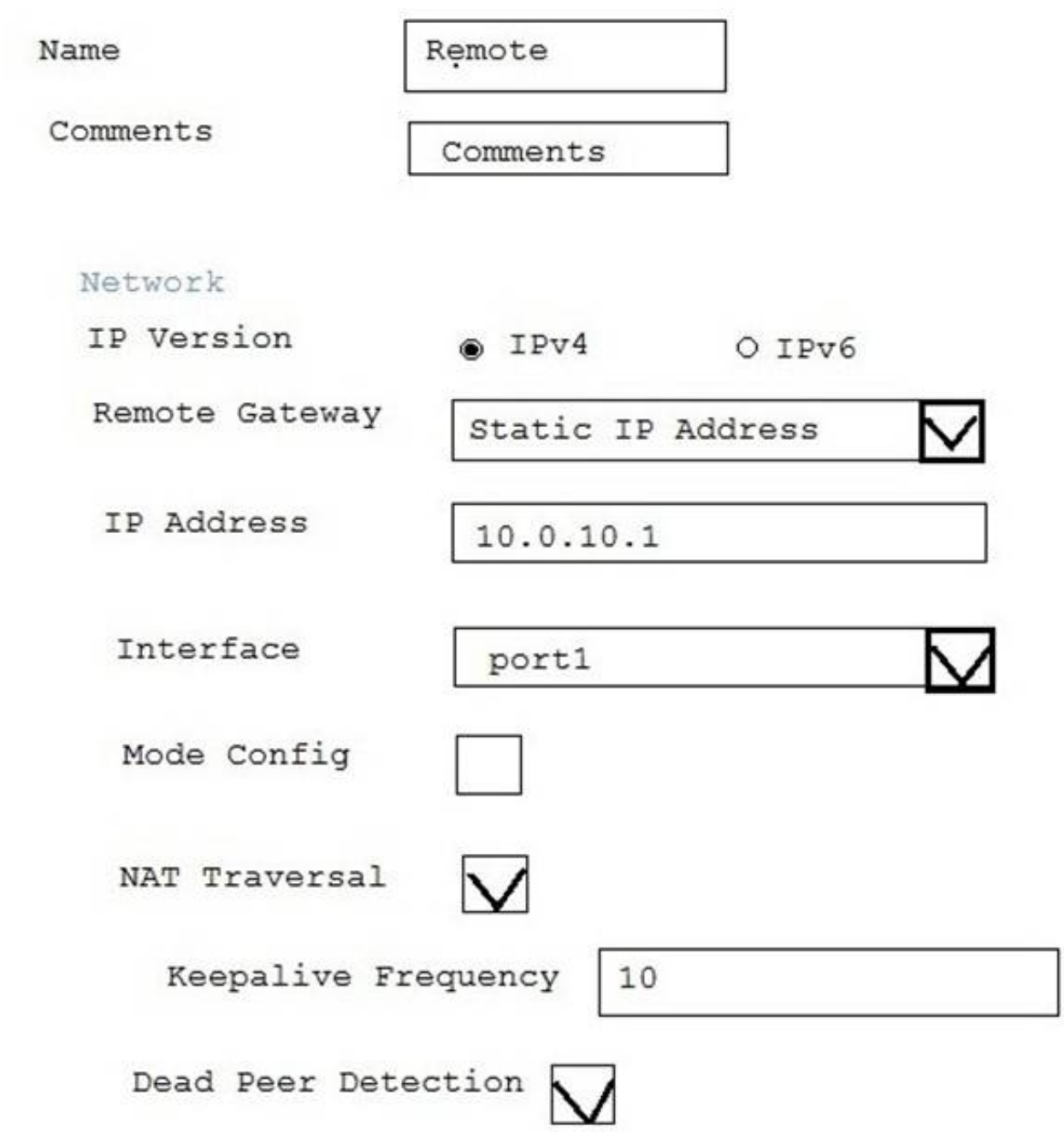
NEW QUESTION 31
A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fsso list' command does not show student as an active FSSO user. Other FSSO 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: BD

NEW QUESTION 36
Examine the IPsec configuration shown in the exhibit; then answer the question below.



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 onl
B. It does not show any more output once the tunnel is up.
C. The log-filter setting is set incorrectl
D. The VPN's traffic does not match this filter.
E. The IKE real time debug shows the phase 1 negotiation onl
F. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
G. The IKE real time debug shows error messages onl
H. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer: A

NEW QUESTION 39
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7....
ike 0: IKEv1 exchange=Aggressive id=baf47d0988e9237f/2f405ef3952f6fda len=430 ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA011004000000000000001AE0400003C000000100000001000000
ike 0:RemoteSite:4: initiator: aggressive mode get 1st response...
ike 0:RemoteSite:4: VID RFC 3947 4A131c81070358455C5728F20E95452F ike 0:RemoteSite:4: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0:RemoteSite:4: peer is FortiGate/Fortios (v5 b727)
ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:RemoteSite:4: received peer identifier FQDN 'remore' ike 0:RemoteSite:4: negotiation result
ike 0:RemoteSite:4: proposal id = 1:
ike 0:RemoteSite:4: protocol id = ISAKMP: ike 0:RemoteSite:4: trans_id = KEY_IKE.
ike 0:RemoteSite:4: encapsulation = IKE/none
ike 0:RemoteSite:4: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key –len=128 ike 0:RemoteSite:4: type=OAKLEY_HASH_ALG, val=SHA.
ike 0:RemoteSite:4: type-AUTH_METHOD, val=PRESHARED_KEY. ike 0:RemoteSite:4: type=OAKLEY_GROUP, val=MODP1024.
ike 0:RemoteSite:4: ISAKMP SA lifetime=86400

ike 0:RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key 16:
B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0:RemoteSite:4: PSK authentication succeeded ike 0:RemoteSite:4: authentication OK
ike 0:RemoteSite:4: add INITIAL-CONTACT
ike 0:RemoteSite:4: enc BAF47D0988E9237F405EF3952F6FDA08100401000000000000000080140000181F2E48BFD8E9D603F
ike 0:RemoteSite:4: out BAF47D0988E9237F405EF3952F6FDA08100401000000000000000008C2E3FC9BA061816A396F009A12
ike 0:RemoteSite:4: sent IKE msg (agg_i2send): 10.0.0.1:500-10.0.0.2:500, len=140, id=baf47d0988e9237f/2 ike 0:RemoteSite:4: established IKE SA
baf47d0988e9237f/2f405ef3952f6fda
Which statements about this debug output are correct? (Choose two.)

A. The remote gateway IP address is 10.0.0.1.
B. It shows a phase 1 negotiation.
C. The negotiation is using AES128 encryption with CBC hash.
D. The initiator has provided remote as its IPsec peer ID.

Answer: BD

NEW QUESTION 44
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

```
# diagnose debug rating
Locale        : english
License       : Contract
Expiration    : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP                Weight   RTT   Flags   TZ   Packets   Curr Lost   Total Lo
69.195.205.101    10       45             -5   262432    0           846
69.195.205.102    10       46             -5   329072    0           6806
209.222.147.43    10       75             -5   71638     0           275
96.45.33.65       20       71             -8   36875     0           92
208.91.112.196    20       103    DI      -8   34784     0           1070
208.91.112.198    20       107    D       -8   35170     0           1533
80.85.69.41       60       144            0    33728     0           120
62.209.40.73      71       226            1    33797     0           192
121.111.236.180   150      197            9    33754     0           145
69.195.205.103    45       44     F       -5   26410     26226       26227
```

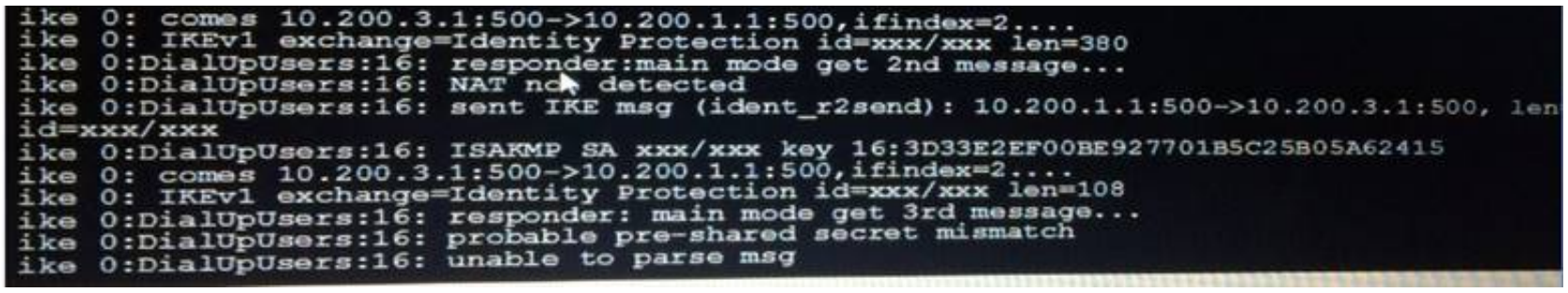
Which statement are true regarding the output in the exhibit? (Choose two.)

A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
B. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
C. FortiGate will send the FortiGuard queries to the server with highest weight.
D. A server's round trip delay (RTT) is not used to calculate its weight.

Answer: BC

NEW QUESTION 46
An administrator added the following Ipsec VPN to a FortiGate configuration:
configvpn ipsec phasel -interface edit "RemoteSite"
set type dynamic
set interface "portl"
set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phasel name "RemoteSite" set proposal 3des-sha256
next end
However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.

```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=716
ike 0:xxx/xxx:16: responder: main mode get 1st message...
ike 0:xxx/xxx:16: VID RFC 3947 4A131C81070358455C5728F20E95452F
...
ike 0:xxx/xxx:16: negotiation result
ike 0:xxx/xxx:16: proposal id = 1:
ike 0:xxx/xxx:16:   protocol id = ISAKMP:
ike 0:xxx/xxx:16:     trans_id = KEY_IKE.
ike 0:xxx/xxx:16:     encapsulation = IKE/none
ike 0:xxx/xxx:16:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:xxx/xxx:16:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:xxx/xxx:16:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:xxx/xxx:16:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:xxx/xxx:16: ISAKMP SA lifetime=86400
ike 0:xxx/xxx:16: SA proposal chosen, matched gateway DialUpUsers
...
ike 0:DialUpUsers:16: sent IKE msg (ident_r1send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
```



What is causing the IPsec problem in the phase 1 ?

A. The incoming IPsec connection is matching the wrong VPN configuration
B. The phrase-1 mode must be changed to aggressive
C. The pre-shared key is wrong
D. NAT-T settings do not match

Answer: C

NEW QUESTION 47
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 refcnt=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  7365e17a8fd555ec38bffa47d650c1a2
       ah=sha1 key=20  946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
  enc: spi=da6d28ac  esp=aes  key=16  3dcf44ac7c816782ea3d0c9a977ef543
       ah=sha1 key=20   7cfde587592fc4635ab8db8ddf0d851d868b243f
dec: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'

Answer: B

NEW QUESTION 52
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: AC

NEW QUESTION 56
A FortiGate's portl is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

A. Both session have the local flag on.
B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
C. One session has the proxy flag on, the other one does not.
D. One of the sessions has the IP address of port2 as the source IP address.

Answer: AD

NEW QUESTION 59
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 sent 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.

Answer: BC

NEW QUESTION 60
View the exhibit, which contains a session entry, and then answer the question below.

```
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(10.200.1.254/10.1.0.1
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 is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Answer: A

NEW QUESTION 64
An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any ‘udp port 500’
B. diagnose sniffer packet any ‘udp port 4500’
C. diagnose sniffer packet any ‘esp’
D. diagnose sniffer packet any ‘udp port 500 or udp port 4500’

Answer: C

NEW QUESTION 69
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: C

NEW QUESTION 70
Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
B. This limit CANNOT be modified by the administrator.
C. FortiGate limits the total number of simultaneous explicit web proxy users.
D. FortiGate limits the number of simultaneous sessions per explicit web proxy use
E. The limit CAN be modified by the administrator.
F. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

Answer: C

NEW QUESTION 71
An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
B. Redirection of HTTP to HTTPS administrative access is disabled.
C. HTTP administrative access is configured with a port number different than 80.
D. The packet is denied because of reverse path forwarding check.

Answer: AC

NEW QUESTION 75
View the exhibit, which contains the output of a web diagnose command, and then answer the question below.

```
# diagnose webfilter fortiguard statistics list

Raring Statistics:
==================================
DNS filures                    :   273
DNS lookups                    :   280
Data send failures             :     0
Data read failures             :     0
Wrong package type             :     0
Hash table miss                :     0
Unknown server                 :     0
Incorrect CRC                  :     0
Proxy requests failures        :     0
Request timeout                :     1
Total requests                 :  2409
Requests to FortiGuard servers :  1182
Server errored responses       :     0
Relayed rating                 :     0
Invalid profile                :     0

Allowed                        :  1021
Blocked                        :  3909
Logged                         :  3927
Blocked Errors                 :   565
Allowed Errors                 :     0
Monitors                       :     0
Authenticates                  :     0
Warnings                       :    18
Ovrd request timeout           :     0
Ovrd send failures             :     0
Ovrd read failures             :     0
Ovrd errored responses         :     0
```

```
# diagnose webfilter fortiguard statistics list

Cache Statistics:
==================================
Maximum memory                 :     0
Memory usage                   :     0

Nodes                          :     0
  Leaves                       :     0
  Prefix nodes                 :     0
  Exact nodes                  :     0

Requests                       :     0
Misses                         :     0
Hits                           :     0
  Prefix hits                  :     0
  Exact hits                   :     0

No cache directives            :     0
Add after prefix               :     0
Invalid DB put                 :     0
DB updates                     :     0

Percent full                   :    0%
  Branches                     :    0%
  Leaves                       :    0%
    Prefix nodes               :    0%
    Exact nodes                :    0%

Miss rate                      :    0%
Hit rate                       :    0%
  Prefix hits                  :    0%
  Exact hits                   :    0%
```

Which one of the following statements explains why the cache statistics are all zeros?

A. The administrator has reallocated the cache memory to a separate process.
B. There are no users making web requests.
C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Answer: D

NEW QUESTION 77
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: D

NEW QUESTION 79
Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

A. 1
B. 2
C. 3
D. 4

Answer: B

NEW QUESTION 80
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.

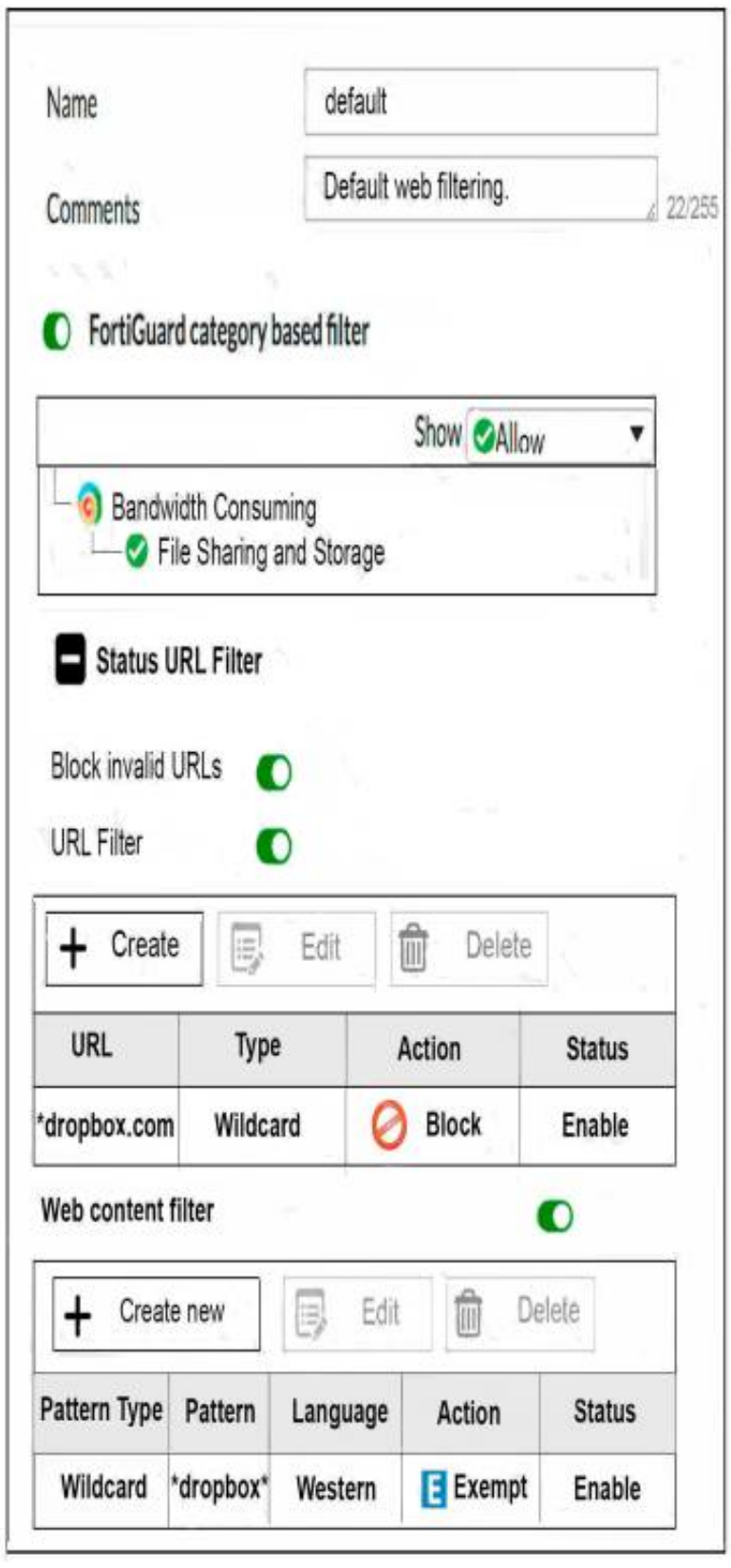
Answer: ABD

NEW QUESTION 81
An administrator has enabled HA session synchronization in a HA cluster with two members. Which flag is added to a primary unit's session to indicate that it has been synchronized to the secondary unit?

A. redir.
B. dirty.
C. synced
D. nds.

Answer: C

NEW QUESTION 84
View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.



Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

A. FortiGate will exempt the connection based on the Web Content Filter configuration.
B. FortiGate will block the connection based on the URL Filter configuration.
C. FortiGate will allow the connection based on the FortiGuard category based filter configuration.
D. FortiGate will block the connection as an invalid URL.

Answer: B

NEW QUESTION 85
What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

A. A process crash.
B. Configuration changes.
C. Changes in the status of any of the FortiGuard licenses.
D. System entering to and leaving from the proxy conserve mode.

Answer: AD

NEW QUESTION 87
View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
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
```

Which one of the following statements is true regarding FortiGate's inspection of this session?

A. FortiGate applied proxy-based inspection.
B. FortiGate forwarded this session without any inspection.
C. FortiGate applied flow-based inspection.
D. FortiGate applied explicit proxy-based inspection.

Answer: B

NEW QUESTION 92
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: BC

NEW QUESTION 93
When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI)?

A. FortiGate uses the Issued To: field in the server's certificate.
B. FortiGate switches to the full SSL inspection method to decrypt the data.
C. FortiGate blocks the request without any further inspection.
D. FortiGate uses the requested URL from the user's web browser.

Answer: D

NEW QUESTION 98
Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

```
#diagnose debug application ike -1
#diagnose debug enable
ike 0: ….: 75: responder: aggressive mode get 1st message…
…
ike 0: ….:76: incoming proposal:
ike 0: ….:76: proposal id = 0:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id = KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type= OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: my proposal, gw Remote:
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id= KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val= PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val =MODP2048.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: proposal id=1:
ike 0: ….:76:    protocol id= ISAKMP:
ike 0: ….:76:      trans_id= KEY_IKE.
ike 0: ….:76:      encapsulation = IKE/none
ike 0: ….:76:        type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: ….:76:        type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ….:76:        type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ….:76:        type=OAKLEY_GROUP, val=MODP1536.
ike 0: ….:76: ISAKMP SA lifetime=86400
ike 0: ….:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0: ….:76: no SA proposal chosen
```

Why didn't the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.
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. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Answer: B

NEW QUESTION 100
Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.
B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.
C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.
D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Answer: AD

NEW QUESTION 105
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7 Product From:

https://www.2passeasy.com/dumps/NSE7/

Money Back Guarantee

NSE7 Practice Exam Features:

* NSE7 Questions and Answers Updated Frequently

* NSE7 Practice Questions Verified by Expert Senior Certified Staff

* NSE7 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year