

Fortinet

Exam Questions NSE7

NSE7 Enterprise Firewall - FortiOS 5.4



NEW QUESTION 1

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=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: 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.

Answer: C

NEW QUESTION 2

Examine the output from the 'diagnose debug authd fssolist' command; then answer the question below.

```
# diagnose debug authd fssolist —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is
```

NOT the one used by the workstation INTERNAL2. TRAINING. LAB.

What should the administrator check?

- A. The IP address recorded in the logon event for the user STUDENT.
- B. The DNS name resolution for the workstation name INTERNAL2. TRAININ
- C. LAB.
- D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ
- E. LAB.
- F. The reserve DNS lookup forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 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 xxxxxxxx
  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: A

NEW QUESTION 4

Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; then 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=39
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
origin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gw=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
serial=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 FortiGuard.
- 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 5

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 6

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: C

NEW QUESTION 7

Examine the following partial output from two system debug commands; then answer the question below.

```
# diagnose hardware sysinfo memory
```

```
MemTotal: 3092728 kB
```

```
MemFree: 1954204 kB
```

```
MemShared: 0 kB
```

```
Buffers: 284 kB
```

```
Cached: 143004 kB
```

```
SwapCached: 0 kB
```

```
Active: 34092 kB
```

```
Inactive: 109256 kB
```

```
HighTotal 1179648 kB
```

```
HighFree: 853516 kB
```

```
LowTotal: 1913080 kB
```

```
LowFree: 1100688 kB
```

```
SwapTotal: 0 kB
```

```
SwapFree: 0 kB
```

```
# diagnose hardware sysinfo shm
```

```
SHM counter: 285
```

```
SHM allocated: 6823936
```

```
SHM total: 623452160
```

```
concermode: 0
```

```
shm last entered: n/a
```

```
system last entered: n/a
```

```
SHM FS total: 639725568
```

```
SHM FS free: 632614912
```

```
SHM FS alloc: 7110656
```

Which of the following statements are true regarding the above outputs? (Choose two.)

- A. The unit is running a 32-bit FortiOS
- B. The unit is in kernel conserve mode
- C. The Cached value is always the Active value plus the Inactive value
- D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Answer: AC

NEW QUESTION 8

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 9

View the exhibit, which contains the output of a BGP debug command, and 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 of the following statements about the exhibit are true? (Choose two.)

- A. For the peer 10.125.0.60, the BGP state of is Established.
- B. The local BGP peer has received a total of three BGP prefixes.
- C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
- D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Answer: BC

NEW QUESTION 10

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: A

NEW QUESTION 10

Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

- A. The next-hop IP address is up.
- B. There is no other route, to the same destination, with a higher distance.
- C. The link health monitor (if configured) is up.
- D. The next-hop IP address belongs to one of the outgoing interface subnets.
- E. The outgoing interface is up.

Answer: ABE

NEW QUESTION 14

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

```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0 10.1.2.254->10.1.1.254
...
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-OFFER): 10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3...
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c
len=196

ike 0:H2S_0_1:15: notify msg received: SHORTCUR-QUERY
ike 0:H2S_0_1: recv shortcut-query 16462343159772385317

ike 0:H2S_0_0:16: senr IKE msg (SHORTCUT-QUERY): 10.200.1.1:500->10.200.3.1:500,
len=196, id=7c6b6cca6700a935/dba061eaf51b89f7:b326df2a
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=3....
ike 0: IKEv1 exchange=Informational id=7c6b6cca6700a935/dba061eaf51b89f7:1c1dbf39
len=188

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc
...
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?

- A. auto-discovery-sender
- B. auto-discovery-forwarder
- C. auto-discovery-shortcut
- D. auto-discovery-receiver

Answer: C

NEW QUESTION 19

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

```
#dia hardware sysinfo shm
SHM counter:          150
SHM allocated:        0
SHM total:            625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:        641236992
SHM FS free:         641208320
SHM FS avail:        641208320
SHM FS alloc:         28672
```

What statement is correct about this FortiGate?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in FD conserve mode.
- C. It is currently in kernel conserve mode because of high memory usage.
- D. It is currently in system conserve mode because of high memory usage.

Answer: D

NEW QUESTION 20

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 25

What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

- A. av-failopen
- B. mem-failopen
- C. utm-failopen
- D. ips-failopen

Answer: A

NEW QUESTION 26

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 28

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 29

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 user The limit CAN be modified by the administrator
- E. 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 34

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
origin->sink: org pre->post, reply pre->post dev=9->3/3->9 gw=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 38

An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created an 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: BDE

NEW QUESTION 40

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=user, dc=trainingAD, dc=training, dc=lab"
    set type regular
    set username "cn=administrator, cn=users, dc=trainingAD,
dc=training, dc=lab"
    set password xxxxx
  next
end
```

The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

```
#diagnose debug application fnbamd -1
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 4 for student in WindowsLDAP
opt=27 prot=0
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_ist_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[1700] fnbamd_ldap_get_result-Error in ldap result: 49
(Invalid credentials)
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 4
fnbamd_fsm.c[568] destroy_auth_session-delete session 4
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the above output, what FortiGate LDAP settings must the administrator check? (Choose two.)

- A. cnid.
- B. username.
- C. password.
- D. dn.

Answer: BC

NEW QUESTION 45

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 48

An administrator cannot connect to the GUI 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 52

What does the dirty flag mean in a FortiGate session?

- A. Traffic has been blocked by the antivirus inspection.
- B. The next packet must be re-evaluated against the firewall policies.
- C. The session must be removed from the former primary unit after an HA failover.
- D. Traffic has been identified as from an application that is not allowed.

Answer: B

NEW QUESTION 53

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 54

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 55

What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

- A. Reduce the session time to live.
- B. Increase the TCP session timers.
- C. Increase the FortiGuard cache time to live.
- D. Reduce the maximum file size to inspect.

Answer: AD

NEW QUESTION 59

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

Name: default
 Comments: Default web filtering. 22/255

FortiGuard category based filter

Show Allow

- Bandwidth Consuming
- File Sharing and Storage

Status URL Filter

Block invalid URLs

URL Filter

+ Create Edit Delete

URL	Type	Action	Status
*dropbox.com	Wildcard	Block	Enable

Web content filter

+ Create new Edit Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	Exempt	Enable

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 63

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 67

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
origin->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 70

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

Answer: C

NEW QUESTION 72

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * NSE7 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7 Practice Test Here](#)