NSE7_EFW-6.0 Q&As

Fortinet NSE 7 - Enterprise Firewall 6.0

Pass Fortinet NSE7_EFW-6.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse7_efw-6-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

```
FGT # diagnose debug rating
Locale        : english
Service       : Web-filter
Status        : Enable
License       : Contract
Service       : Antispam
Status        : Disable
Service       : Virus Outbreak Prevention
Status        : Disable
 -=- Server List (Mon Apr 19  10:41:32 20xx) -=-
IP                   Weight   RTT      Flags     TZ   Packets   Curr Lost     Total Lost
64.26.151.37         10       45                 -5   262432    0             846
64.26.151.35         10       46                 -5   329072    0             6806
66.117.56.37         10       75                 -5   71638     0             275
65.210.95.240        20       71                 -8   36875     0             92
209.222.147.36       20       103      DI        -8   34784     0             1070
208.91.112.194       20       107      D         -8   35170     0             1533
96.45.33.65          60       144                 0   33728     0             120
80.85.69.41          71       226                 1   33797     0             192
62.209.40.74         150      97                  9   33754     0             145
121.111.236.179      45       44       F         -5   26410     26226         26227
```

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

A. FortiGate used 209.222.147.36 as the initial server to validate its contract.

B. Servers with the D flag are considered to be down.

C. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.

D. Servers with a negative TZ value are experiencing a service outage.

Correct Answer: AC

QUESTION 2

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filler web requests when the client browser does not provide the server name indication (SNI) extension ?

A. FortiGate switches to the full SSL inspection method to decrypt the data.

B. FortiGate blocks the request without any further inspection.

C. FortiGate uses the Issued T: field in the server\\'s certificate.

D. FortiGate uses the requested URL from the user\\'s web browser.

Correct Answer: C

QUESTION 3

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

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 sent 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

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

A. Port4 is connected to the OSPF backbone area.

B. In the network connected to port4, two OSPF routers are down.

C. The local FortiGate is the backup designated router.

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

Correct Answer: AD

QUESTION 4

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

```
# diagnose webfilter fortiguard statistics list

Rating Statistics:
==================
DNS failures                    :        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 request 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. There are no users making web requests.

B. The administrator has reallocated the cache memory to a separate process.

C. The FortiGuard web filter cache is disabled in the FortiGate\\'s configuration.

D. FortiGate is using flow-based inspection which doesn\\'t use the cache.

Correct Answer: C

QUESTION 5

View the exhibit, which contains a session table entry, and then answer the question below.

```
FGT = diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=redir local may_dirty none app_ntf
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=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)
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
rpdb_link_id = 00000000
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 FortiGates\\'s inspection of this session?

A. FortiGate applied flow-based inspection.

B. FortiGate applied proxy-based inspection.

C. FortiGate forwarded this session without any inspection.

D. FortiGate applied NGFW flow-based inspection.

Correct Answer: B