Fortinet

Exam NSE7

Fortinet Troubleshooting Professional

Version: 8.0

[Total Questions: 30]

Question No : 1

Examine the output of the 'diagnose debug rating' commandshown 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 Los
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 valuerepresents 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: B,C

Question No : 2

A FortiGate's portl is connected to a private network. Its port2 is connected to the Internet. Explicit webproxy 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 FortiGatesession 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'sinterfaces.
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: A,D

Question No : 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: B

Question No : 4

Examine the following traffic log; then answer the question below.

**date-20xx-02-01 time=19:52:01 devname=masterdevice_id="xxxxxxx"
log_id=0100020007 type=event subtype=system pri critical vd=root service=kemel
status=failure msg="NAT port is exhausted."**

What does the log mean?

A. There is not enough available memory in the system to create a new entry in the NAT port table.