

Fortinet

Exam NSE7

NSE7 Enterprise Firewall - FortiOS 5.4

Verson: Demo

[Total Questions: 10]

Question No : 1

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

Question No : 2

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

Question No : 3

Which the following events can trigger the election of a new primary unit in a HA cluster?
(Choose two.)

- A. Primary unit stops sending HA heartbeat *keepalives*.
- B. The FortiGuard license for the primary unit is updated.
- C. One of the monitored interfaces in the primary unit is disconnected.
- D. A secondary unit is removed from the HA cluster.

Answer: A,B

Question No : 4

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

Question No : 5

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: A,D

Question No : 6

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 Lost
69.195.205.101  10     45    -S     -5   262432   0          846
69.195.205.102  10     46    -S     -5   329072   0          6806
209.222.147.43  10     75    -S     -5   71638    0          275
96.45.33.65    20     71    -S     -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      0    33728    0          120
62.209.40.73   71     226   1      1    33797    0          192
121.111.236.180 150    197   9      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: B,C

Question No : 7

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: A,C

Question No : 8

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

- A. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Answer: C,D

Question No : 9

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

Question No : 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: C