

IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

Exam : **NSE7_EFW-6.0**

Title : Fortinet NSE 7 - Enterprise
Firewall 6.0

Version : DEMO

1.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

2.View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which one of the following statements about the output is true?

- A. This session is for HA heartbeat traffic.
- B. This session cannot be synced with the slave unit.
- C. The master unit is processing this traffic.
- D. The inspection of this session has been offloaded to the slave unit.

Answer: C

3.Which of the following tasks are automated using the Install Wizard on FortiManager? (Choose two.)

- A. Install configuration changes to managed devices.
- B. Preview pending configuration changes for managed devices.
- C. Import policy packages from managed devices.
- D. Add devices to FortiManager.
- E. Import interface mappings from managed devices

Answer: A,B

4.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
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)
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
rpd_b_link_id = 00000000
dd_type=0 dd_mode=0
np_u_state=00000000
np_u_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 flow-based inspection.
- B. FortiGate applied proxy-based inspection.
- C. FortiGate forwarded this session without any inspection.
- D. FortiGate applied NGFW flow-based inspection.

Answer: B

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

```

FGT # 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
100.64.3.1    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. The local router's BGP state is Established with the 10.125.0.60 peer.

- B. Since the counters were last reset; the 10.200.3.1 peer has never been down.
- C. The local router has received a total of three BGP prefixes from all peers.
- D. The local router has not established a TCP session with 100.64.3.1.

Answer: A,D