NSE7_EFW Q&As

NSE7 Enterprise Firewall - FortiOS 5.4

Pass Fortinet NSE7_EFW Exam with 100% Guarantee

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

https://www.passapply.com/nse7_efw.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

```
diagnose sys session list expectation

session info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-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
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=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
```

What statements are correct regarding the output? (Choose two.)

A. This is an expected session created by a session helper.

B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.

C. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.

D. This is an expected session created by an application control profile.

Correct Answer: AC

QUESTION 2

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.

Correct Answer: C

QUESTION 3

Examine the output of the `get router info bgp summary\\' command shown in the exhibit; 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
```

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

A. BGP state of the peer 10.125.0.60 is Established.

B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.

C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.

D. The local BGP peer has received a total of 3 BGP prefixes.

Correct Answer: AC

QUESTION 4

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 refent=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
       ag=sha1 key=20 946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
   enc:spi=da6d28ac esp=aes key=16 3dcf44ac7c816782ea3d0c9a977ef543
       ah=sha1 key=20 7cfdc587592fc4635ab8db8ddf0d851d868b243f
   dcc: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\\'

Correct Answer: B

QUESTION 5

The CLI command set intelligent-mode controls the IPS engine\\'s adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

A. Determines the optimal number of IPS engines required based on system load.

B. Downloads signatures on demand from FDS based on scanning requirements.

C. Determines when it is secure enough to stop scanning session traffic.

D. Choose a matching algorithm based on available memory and the type of inspection being performed.

Correct Answer: D