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.passapply.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

Which of the following statements are correct regarding application layer test commands? (Choose two.)

A. Some of them display statistics and configuration information about a feature or process.

B. They are used to filter real-time debugs.

C. They display real-time application debugs.

D. Some of them can be used to restart an application.

Correct Answer: AD

QUESTION 2

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.

Correct Answer: AD

QUESTION 3

View the global IPS configuration, and then answer the question below.

```
config ips global
     set fail-open disable
     set intelligent-mode disable
     set cp-accel-mode advanced
     set engine-count 0
end
```

Which of the following statements is true regarding this configuration? (Choose two.)

A. IPS will scan every byte in every session.

B. IPS acceleration is disabled in this FortiGate device\\'s configuration.

C. New packets requiring IPS inspection will be passed through during conserve mode.

D. FortiGate will spawn IPS engine instances based on the system load.

Correct Answer: AD

QUESTION 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
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

QUESTION 5

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any \\'esp\\'

B. diagnose sniffer packet any \\'tcp port 500 or tcp port 4500\\'

C. diagnose sniffer packet any \\'udp port 4500\\'

D. diagnose sniffer packet any \\'udp port 500\\'

Correct Answer: A