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 global IPS configuration, and then answer the question below.

```
config ips global
   set fail-open disable
   set intelligent-mode disable
   set engine-count 0
   set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

A. IPS will scan every byte in every session.

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

C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.

D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Correct Answer: A

QUESTION 2

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.

Correct Answer: A

QUESTION 3

Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

A. The next-hop IP address is up.

B. There is no other route, to the same destination, with a higher distance.

C. The link health monitor (if configured) is up.

D. The next-hop IP address belongs to one of the outgoing interface subnets.

E. The outgoing interface is up.

Correct Answer: ABE

QUESTION 4

Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Correct Answer: AD

QUESTION 5

View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.

B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.

C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.

D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Correct Answer: A