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.pass4itsure.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

Examine the following partial outputs from two routing debug commands; then answer the question below.

get router info kernel

tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0

gwy=10.200.1.254 dev=2(port1)

tab=254 vf=0 scope=0type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0

gwy=10.200.2.254 dev=3(port2)

tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254

gwy=0.0.0.0 dev=4(port3)

get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, portl [10/0] via 10.200.2.254, port2,

[10/0] dO.0.1.0/24 is directly connected, port3 dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is

directly connected, port2 Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!

B. port2.

C. Both portl and port2.

D. port3.

Correct Answer: B

QUESTION 2

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

QUESTION 3

What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

A. av-failopen

B. mem-failopen

C. utm-failopen

D. ips-failopen

Correct Answer: A

QUESTION 4

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 `udp port 500\\'

B. diagnose sniffer packet any `udp port 4500\\'

C. diagnose sniffer packet any `esp\\'

D. diagnose sniffer packet any `udp port 500 or udp port 4500\\'

Correct Answer: C

QUESTION 5

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