Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://tw.fast2test.com

高效的考試材料是最高通過率的考試題庫

Exam : **NSE7_EFW**

Title : NSE7 Enterprise Firewall - FortiOS 5.4

Vendor : Fortinet

Version : DEMO

NO.1 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 was detected as an anomaly by an IPS sensor.

B. Those whose traffic matches a DoS policy.

C. Those whose traffic exceeded a threshold of a matching DoS policy.

D. Those whose traffic matches an IPS sensor.

Answer: B

NO.2 Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-miltipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

TheBGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

A. Enable the setting ebgp-multipath.

B. Enable the redistribution of static routers into BGP.

C. Disable the setting network-import-check.
D. Enable the redistribution of connected routers into BGP.
Answer: C

NO.3 Which configuration can be used to reduce the number of BGP sessions in an IBGP network?
A. Neighbor range
B. Next-hop-self
C. Neighbor group
D. Route reflector
Answer: D

NO.4 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 CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.
D. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
Answer: A

NO.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 'udp port 4500'
B. diagnose sniffer packet any 'esp'
C. diagnose sniffer packet any 'udp port 500 or udp port 4500'
D. diagnose sniffer packet any 'udp port 500'
Answer: B

NO.6 Examine the output of the 'get router info ospf interface' command shown in the exhibit; then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address
172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit
5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

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

A. The local FortiGate has been elected as the OSPF backup designated router.

B. There are at least 5 OSPF routers connected to the port4 network.

C. Two OSPF routers are down in the port4 network.

D. The port4 interface is connected to the OSPF backbone area.

Answer: C,D

NO.7 Examine the following partial outputs from two routing debug commands; then answer the question below:

```
#get router info routing-table database
S       0.0.0.0/. [20/0] via 10.200.2.254, port2, [10/0]
S       *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

Why the default route using port2 is not displayed in the output of the second command?

A. It has a higher distance than the default route using port1.

B. It has a lower priority than the default route using port1.

C. It is disabled in the FortiGate configuration.

D. It has a higher priority than the default route using port1.

Answer: B

NO.8 Which of the following statements are true about FortiManager when it is deployed as a local FDS? (Choose two.)

A. Supports rating requests from both managed and unmanaged devices.

B. Caches available firmware updates for unmanaged devices.

C. Provides VM license validation services.

D. Can be configured as an update server, or a rating server, but not both.

Answer: B,C