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.geekcert.com/nse7_efw.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

View these partial outputs from two routing debug commands:

```
# get router info kernel
tab=254 vf=0 scope=0 type=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=0 type=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=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 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, port1
                  [10/0] via 10.200.2.254, port2, [10/0]
c       10.0.1.0/24 is directly connected, port3
c       10.200.1.0/24 is directly connected, port1
c       10.200.2.0/24 is directly connected, port2
```

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

A. Both port1 and port2

B. port3

C. port1

D. port2

Correct Answer: C

QUESTION 2

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 3

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below: Which statements are true regarding the output in the exhibit? (Choose two.)

```
#   diagnose ip router bgp all enable
#   diagnose ip router bgp level info
#   diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byt
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

A. BGP peers have successfully interchanged Open and Keepalive messages.

B. Local BGP peer received a prefix for a default route.

C. The state of the remote BGP peer is OpenConfirm.

D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Correct Answer: AB

QUESTION 4

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 5

Examine the output from the \\'diagnose debug authd fsso list\\' command; then answer the question below.

diagnose debug authd fsso list --FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is NOT the one used by the workstation INTERNAL2. TRAINING. LAB.

What should the administrator check?

A. The IP address recorded in the logon event for the user STUDENT.

B. The DNS name resolution for the workstation name INTERNAL2. TRAINING. LAB.

C. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2. TRAINING. LAB.

D. The reserve DNS lookup forthe IP address 192.168.3.1.

Correct Answer: C

NSE7_EFW Study Guide   NSE7_EFW Exam   NSE7_EFW Braindumps
                                Questions