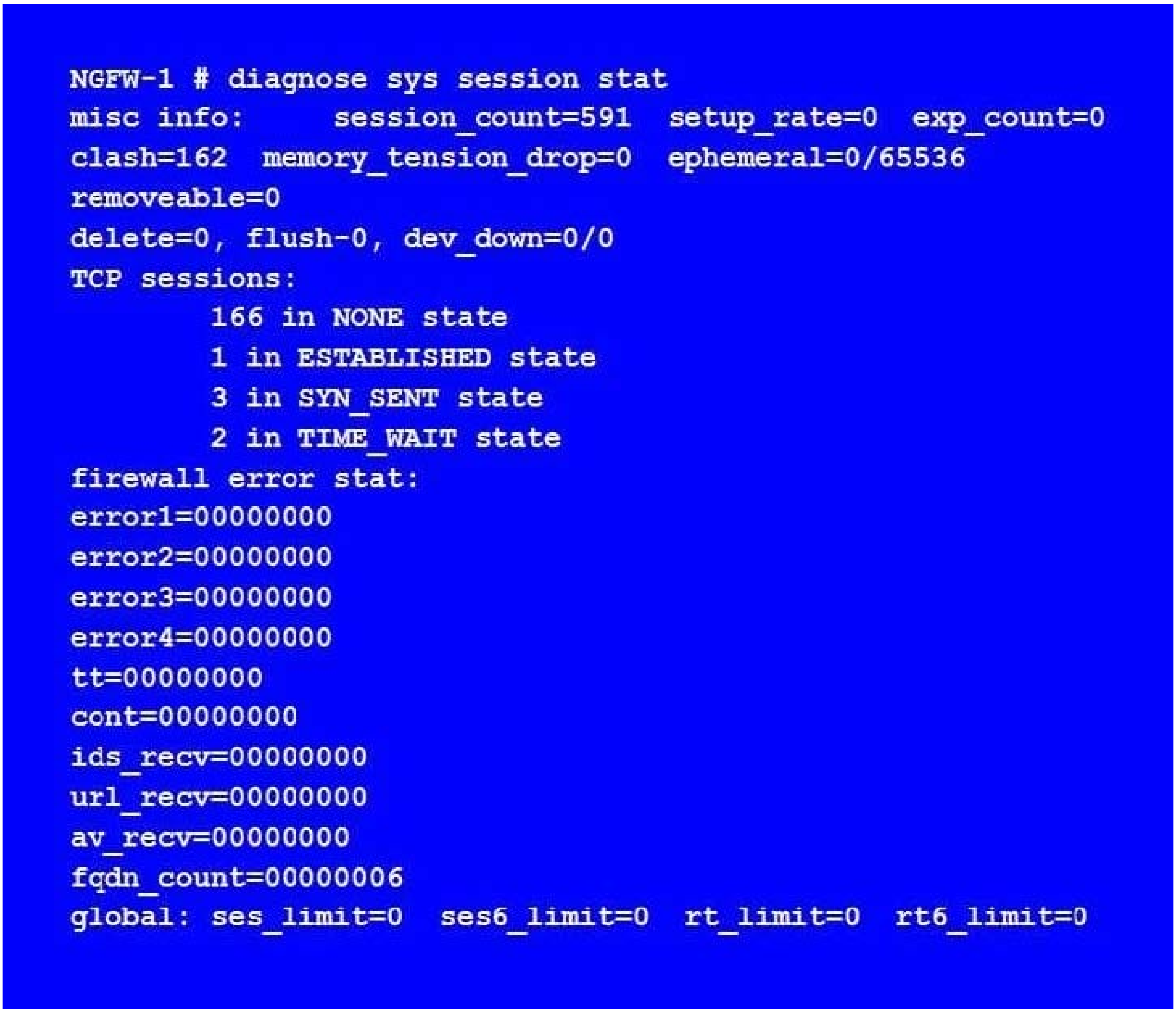
NSE7_EFW-6.2$^{Q\&As}$

Fortinet NSE 7 - Enterprise Firewall 6.2

Pass Fortinet NSE7_EFW-6.2 Exam with 100% Guarantee

QUESTION 1

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.



```
NGFW-1 # diagnose sys session stat
misc info:     session_count=591  setup_rate=0  exp_count=0
clash=162  memory_tension_drop=0  ephemeral=0/65536
removeable=0
delete=0, flush-0, dev_down=0/0
TCP sessions:
        166 in NONE state
        1 in ESTABLISHED state
        3 in SYN_SENT state
        2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
global: ses_limit=0  ses6_limit=0  rt_limit=0  rt6_limit=0
```

Which statements are correct regarding the output shown? (Choose two.)

A. There are 0 ephemeral sessions.

B. All the sessions in the session table are TCP sessions.

C. No sessions have been deleted because of memory pages exhaustion.

D. There are 166 TCP sessions waiting to complete the three-way handshake.

Correct Answer: AC

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578

QUESTION 2

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

Capture IKE Traffic without NAT:

diagnose sniffer packet `host and udp port 500\\'

-- Capture ESP Traffic without NAT:

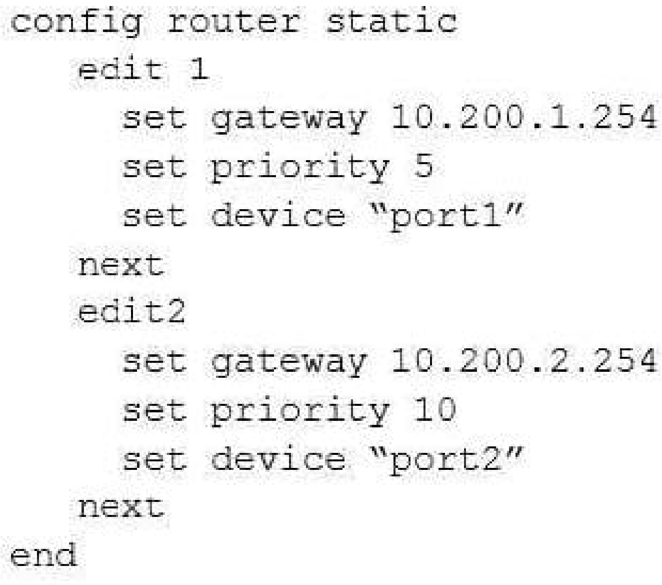
diagnose sniffer packet any `host and esp\\'

-- Capture IKE and ESP with NAT-T:

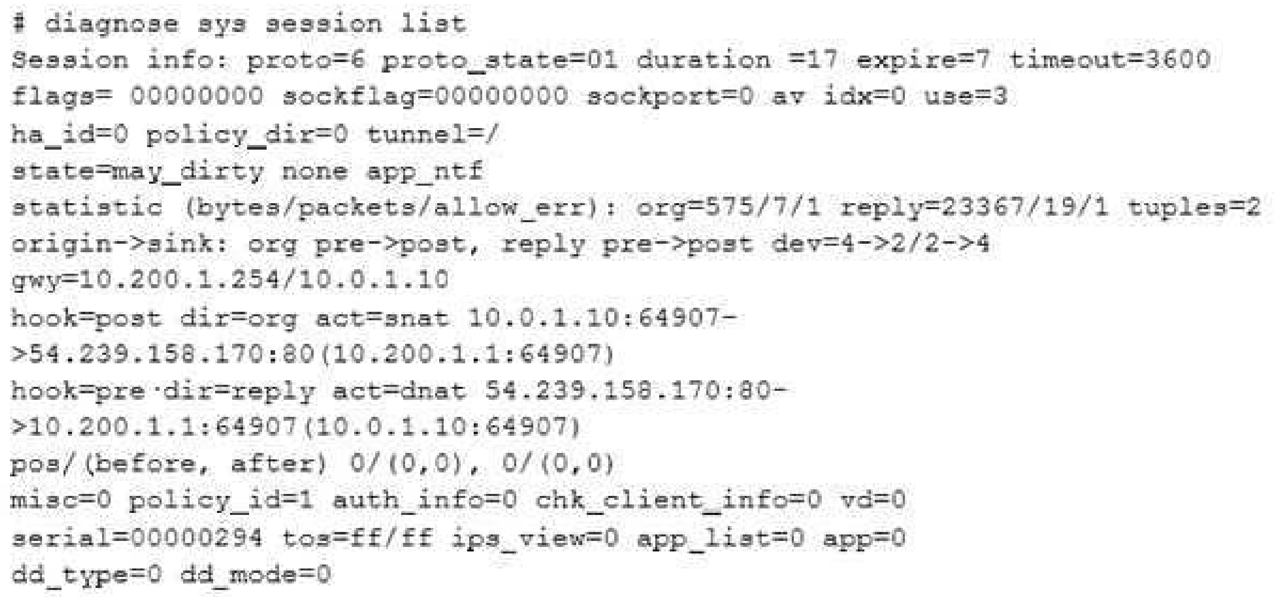
diagnose sniffer packet any `host and (udp port 500 or udp port 4500)\\'

QUESTION 3

A FortiGate has two default routes: All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:



```
config router static
   edit 1
      set gateway 10.200.1.254
      set priority 5
      set device “port1”
   next
   edit2
      set gateway 10.200.2.254
      set priority 10
      set device “port2”
   next
end
```



```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.

B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.

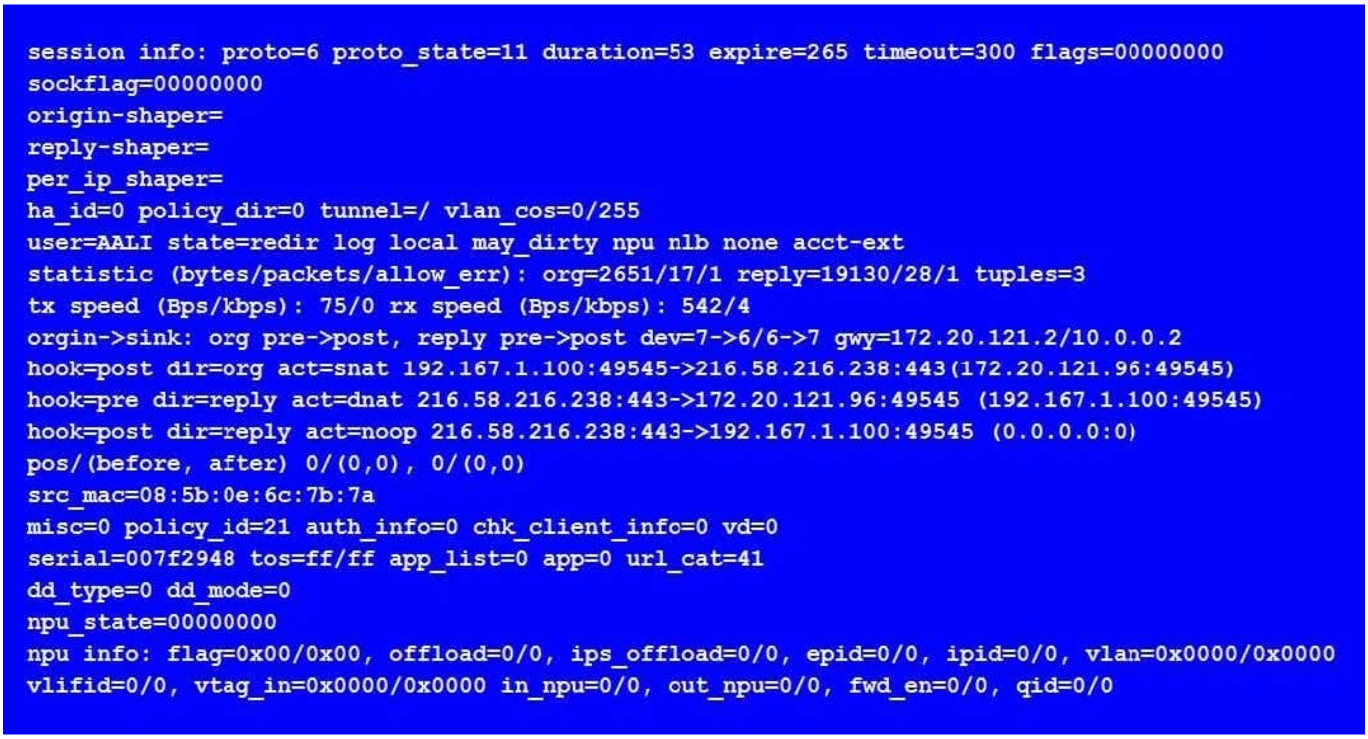
C. Session would be deleted, so the client would need to start a new session.

D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Correct Answer: A

QUESTION 4

View the exhibit, which contains an entry in the session table, and then answer the question below.



```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
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)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
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
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 FortiGate\\'s inspection of this session?

A. FortiGate applied proxy-based inspection.

B. FortiGate forwarded this session without any inspection.

C. FortiGate applied flow-based inspection.

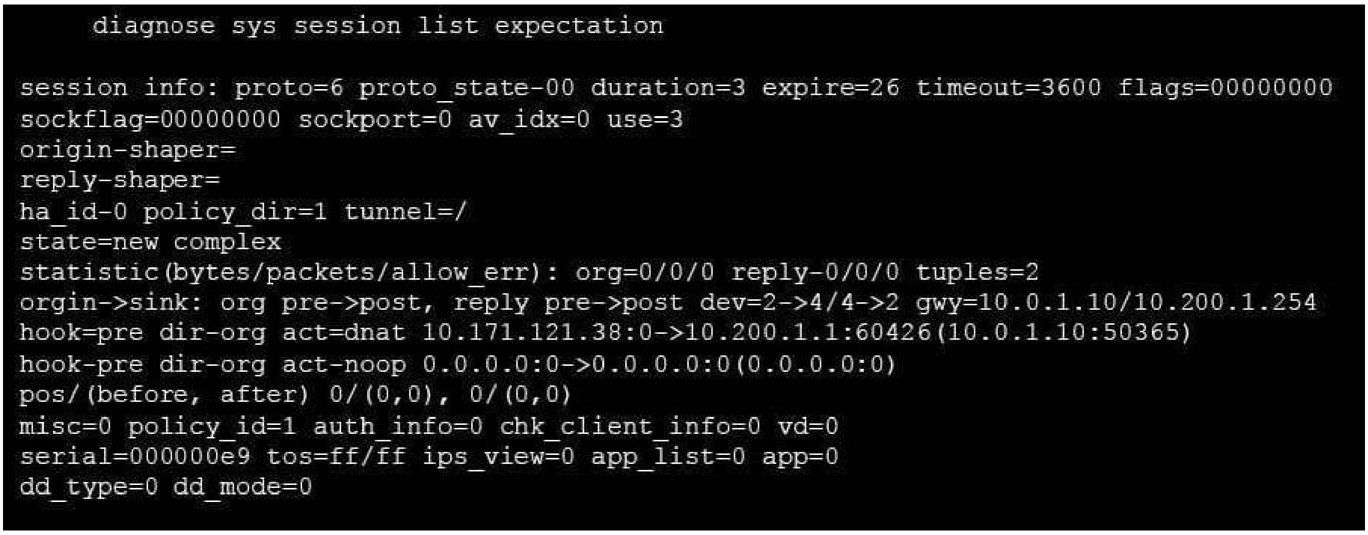
D. FortiGate applied explicit proxy-based inspection.

Correct Answer: A

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

QUESTION 5

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

[Latest NSE7_EFW-6.2 Dumps](https://www.geekcert.com/nse7_efw-6-2.html) [NSE7_EFW-6.2 Practice Test](https://www.geekcert.com/nse7_efw-6-2.html) [NSE7_EFW-6.2 Exam Questions](https://www.geekcert.com/nse7_efw-6-2.html)