FCNSP.V5$^{Q\&As}$

Fortinet Certified Network Security Professional (FCNSP.v5)

QUESTION 1

The following diagnostic output is displayed in the CLI:

diag firewall auth list

policy iD. 9, srC. 192.168.3.168, action: accept, timeout: 13427 user: forticlient_chk_only, group: flag (80020): auth timeout_ext, flag2 (40): exact group iD. 0, av group: 0 ----- 1 listed, 0 filtered -----

Based on this output, which of the following statements is correct?

A. Firewall policy 9 has endpoint compliance enabled but not firewall authentication.

B. The client check that is part of an SSL VPN connection attempt failed.

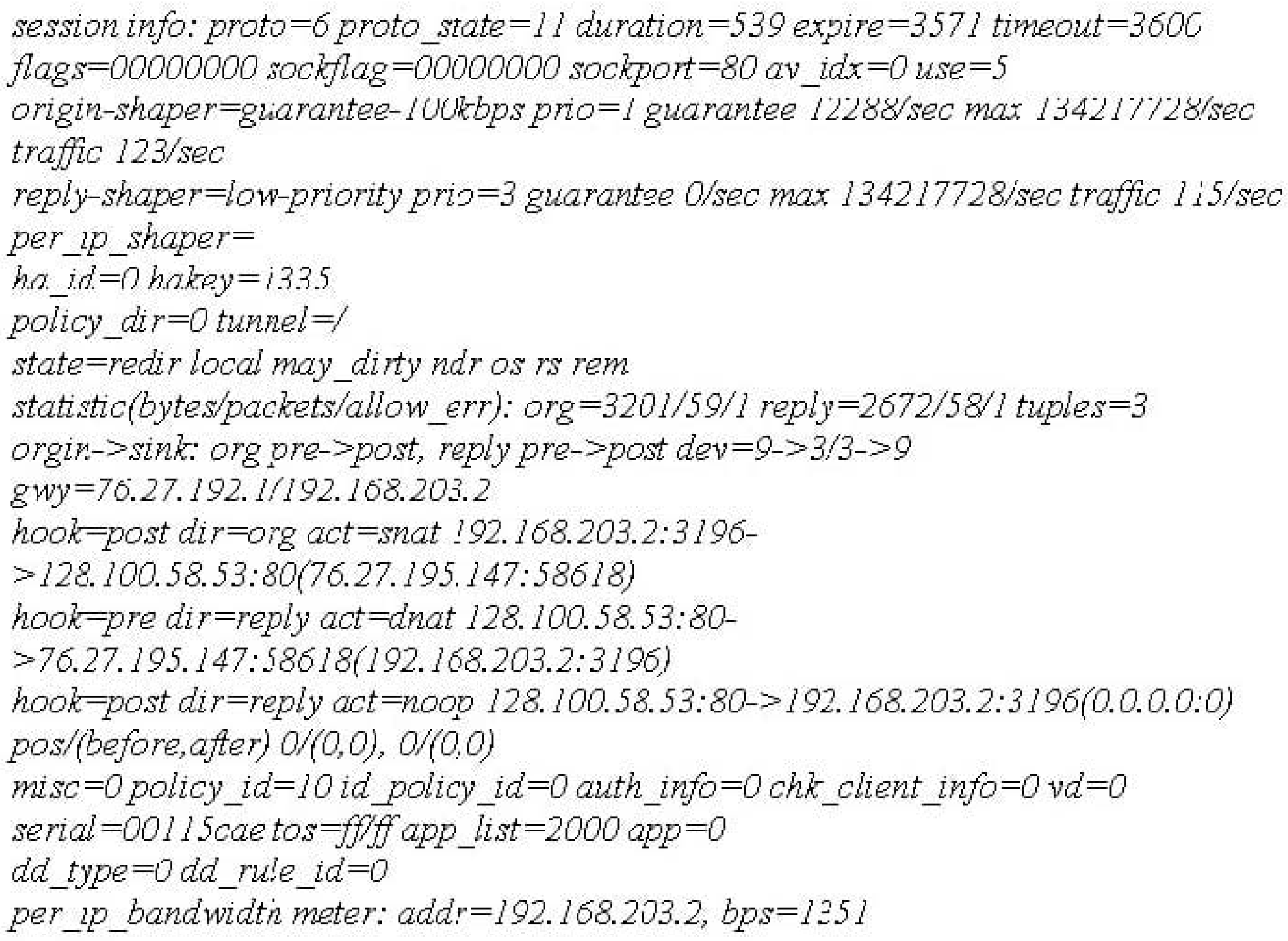
C. This user has been associated with a guest profile as evidenced by the group id of 0.

D. An auth-keepalive value has been enabled.

Correct Answer: A

QUESTION 2

The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.



```
session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=ff/ff app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351
```

Based on the output from this command, which of the following statements is correct?

A. This is a UDP session.

B. Traffic shaping is being applied to this session.

C. This is an ICMP session.

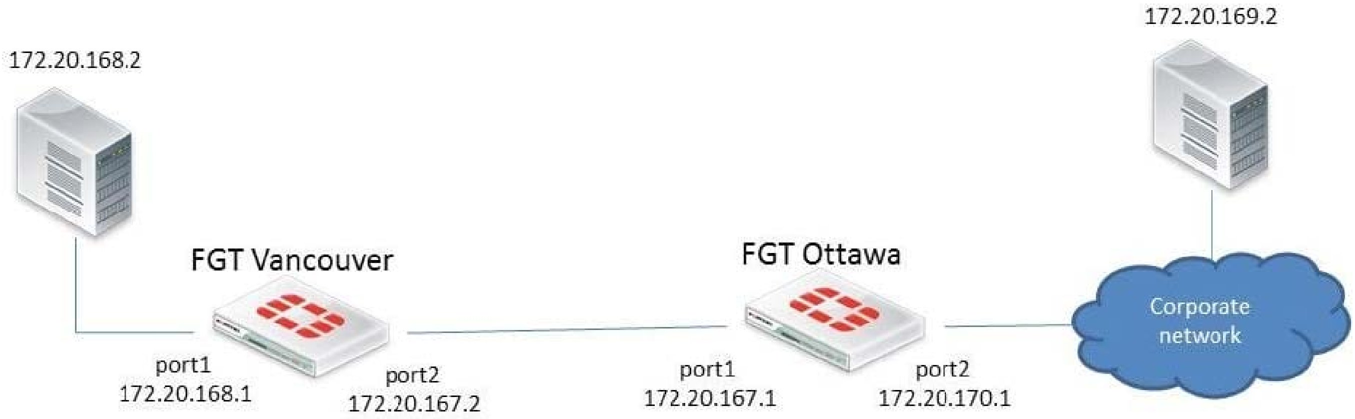
D. This traffic has been authenticated.

E. This session matches a firewall policy with ID 5.

Correct Answer: B

QUESTION 3

Examine the Exhibit shown below; then answer the question following it.



In this scenario, the Fortigate unit in Ottawa has the following routing table: S* 0.0.0.0/0 [10/0] via 172.20.170.254, port2 C 172.20.167.0/24 is directly connected, port1 C 172.20.170.0/24 is directly connected, port2

Sniffer tests show that packets sent from the Source IP address 172.20.168.2 to the Destination IP address 172.20.169.2 are being dropped by the FortiGate unit located in Ottawa. Which of the following correctly describes the cause for the dropped packets?

A. The forward policy check.

B. The reverse path forwarding check.

C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate unit\\'s routing table.

D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Correct Answer: B

QUESTION 4

Review the CLI configuration below for an IPS sensor and identify the correct statements regarding this configuration from the choices below. (Select all that apply.)

config ips sensor edit "LINUX_SERVER" set comment \\'\\' set replacemsg-group \\'\\' set log enable config entries edit 1 set action default set application all set location server set log enable set log-packet enable set os Linux set protocol all set quarantine none set severity all set status default next end next end

A. The sensor will log all server attacks for all operating systems.

B. The sensor will include a PCAP file with a trace of the matching packets in the log message of any matched signature.

C. The sensor will match all traffic from the address object `LINUX_SERVER\\'.

D. The sensor will reset all connections that match these signatures.

E. The sensor only filters which IPS signatures to apply to the selected firewall policy.

Correct Answer: BE

QUESTION 5

Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code

B. TCP/UDP source and destination ports

C. IP protocol number

D. TCP sequence number

Correct Answer: D