NSE8_811$^{\text{Q\&As}}$

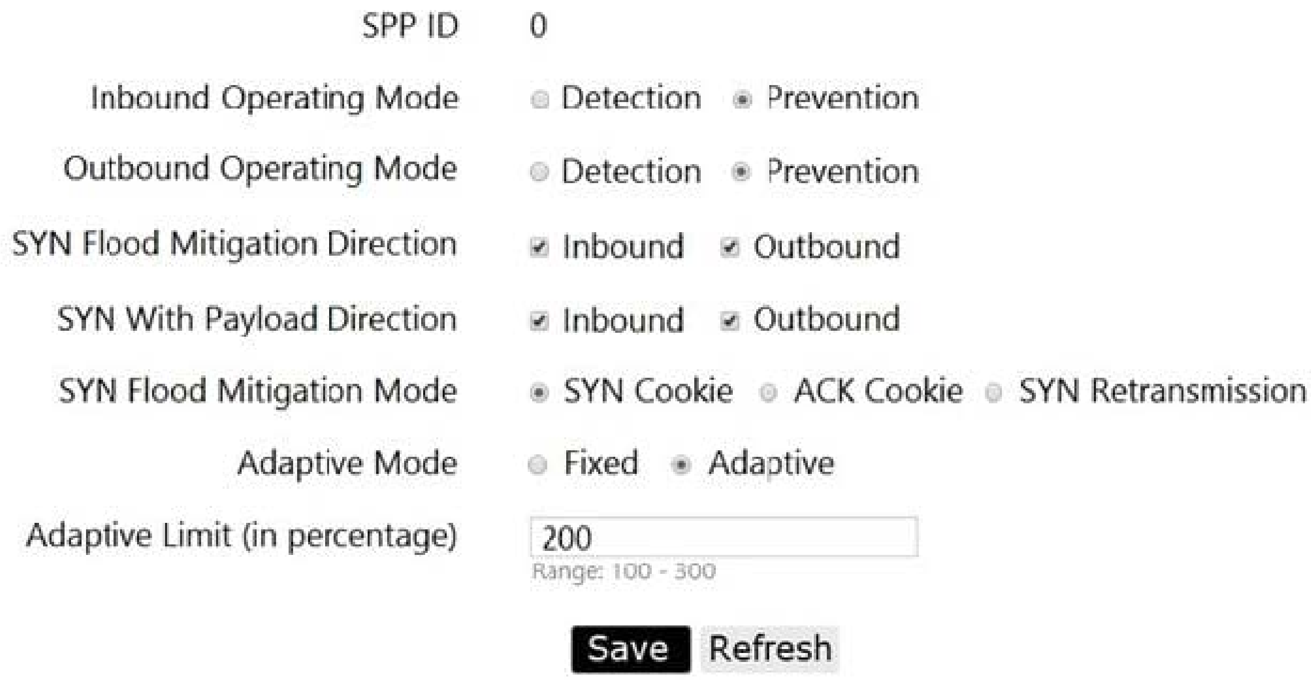
Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.



SPP ID	0
Inbound Operating Mode	○ Detection ● Prevention
Outbound Operating Mode	○ Detection ● Prevention
SYN Flood Mitigation Direction	☑ Inbound ☑ Outbound
SYN With Payload Direction	☑ Inbound ☑ Outbound
SYN Flood Mitigation Mode	● SYN Cookie ○ ACK Cookie ○ SYN Retransmission
Adaptive Mode	○ Fixed ● Adaptive
Adaptive Limit (in percentage)	200 Range: 100 - 300

The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device. Which two statements are true about the traffic matching being inspected by this SPP? (Choose two.)

A. Traffic that does not match any SPP policy will be inspected by this SPP.

B. FortiDDoS will not send a SYN/ACK if a SYN packet is coming from an IP address that is not in the legitimate IP (LIP) address table.

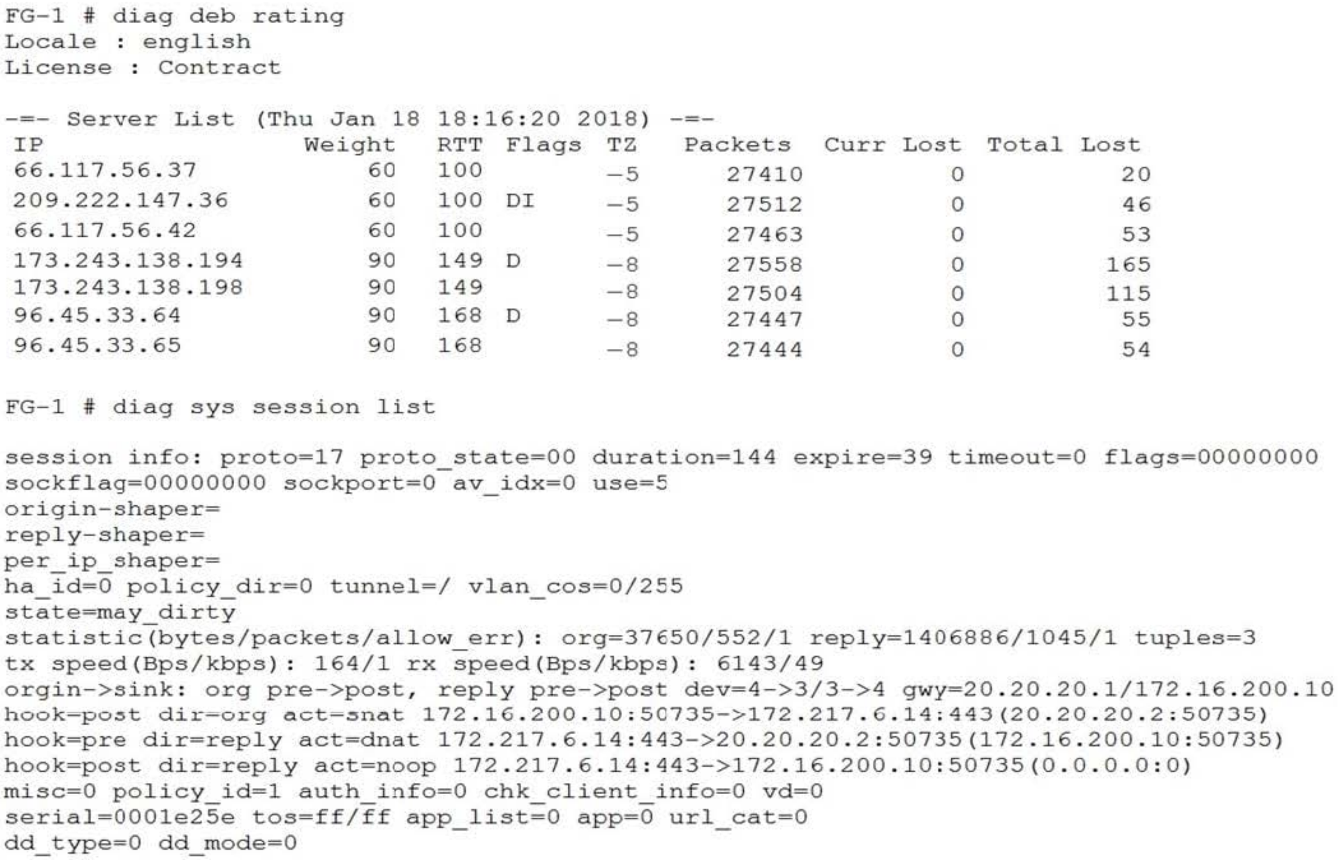
C. FortiDDoS will start dropping packets as soon as the traffic exceeds the configured minimum threshold.

D. SYN packets with payloads will be dropped.

Correct Answer: AD

QUESTION 2

Refer to the exhibit.



```
FG-1 # diag deb rating
Locale : english
License : Contract

-=- Server List (Thu Jan 18 18:16:20 2018) -=-
 IP                    Weight  RTT Flags  TZ   Packets  Curr Lost  Total Lost
 66.117.56.37              60  100        -5     27410          0          20
 209.222.147.36            60  100  DI    -5     27512          0          46
 66.117.56.42              60  100        -5     27463          0          53
 173.243.138.194           90  149  D     -8     27558          0         165
 173.243.138.198           90  149        -8     27504          0         115
 96.45.33.64               90  168  D     -8     27447          0          55
 96.45.33.65               90  168        -8     27444          0          54

FG-1 # diag sys session list

session info: proto=17 proto_state=00 duration=144 expire=39 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=5
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=37650/552/1 reply=1406886/1045/1 tuples=3
tx speed(Bps/kbps): 164/1 rx speed(Bps/kbps): 6143/49
orgin->sink: org pre->post, reply pre->post dev=4->3/3->4 gwy=20.20.20.1/172.16.200.10
hook=post dir=org act=snat 172.16.200.10:50735->172.217.6.14:443(20.20.20.2:50735)
hook=pre dir=reply act=dnat 172.217.6.14:443->20.20.20.2:50735(172.16.200.10:50735)
hook=post dir=reply act=noop 172.217.6.14:443->172.16.200.10:50735(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0001e25e tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

You configured AV and Web filtering for your outgoing Internet connections. You later notice that not all Web sessions are being inspected and you start troubleshooting the problem.

Referring to the exhibit, what can be causing this problem?

A. The Web session is using QUIC which is not inspected by the FortiGate.

B. There are problems with the connection to the Web filter servers, therefore the Web session cannot be categorized.

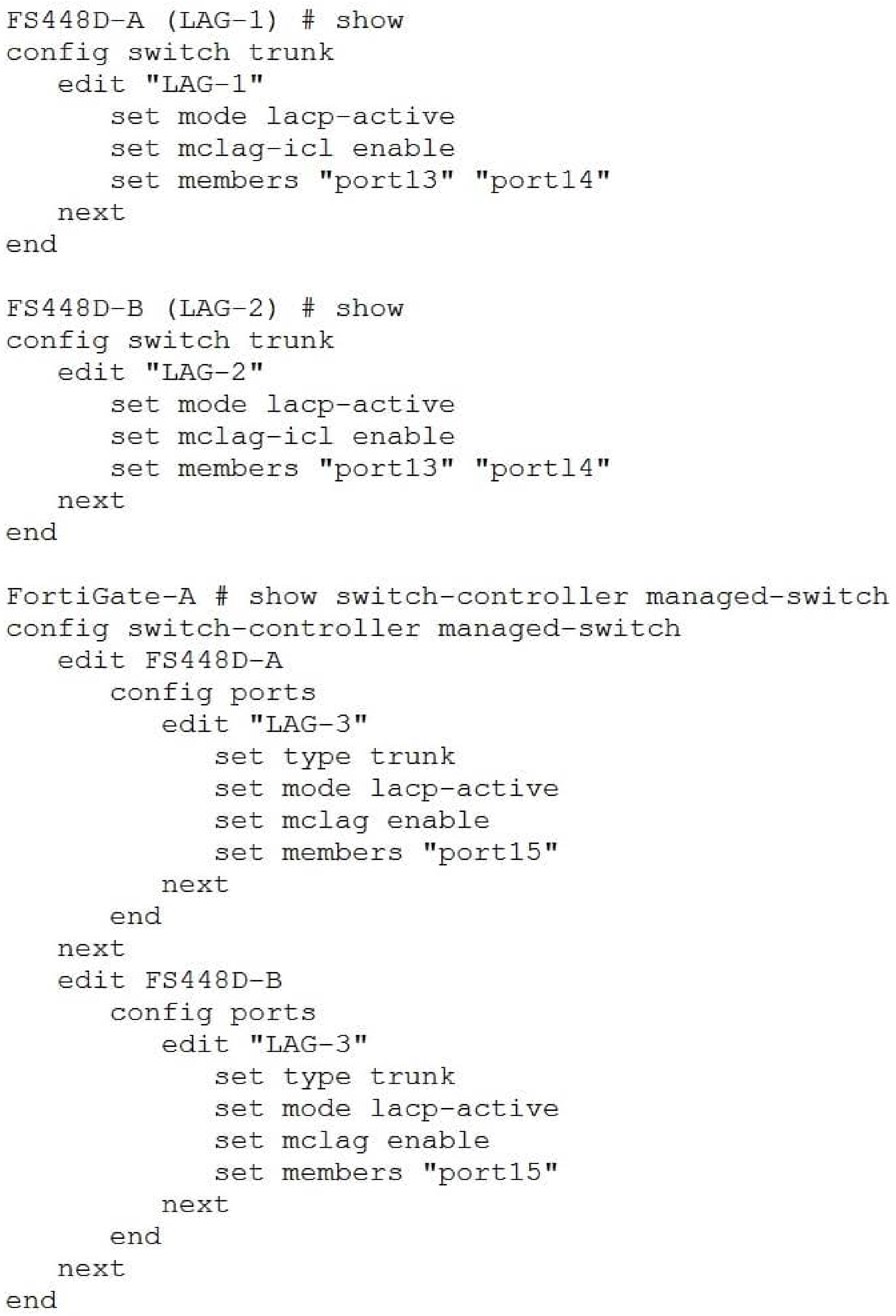
C. The SSL inspection options are not set to deep inspection.

D. Web filtering is not licensed; therefore, no inspection occurs.

Correct Answer: A

QUESTION 3

Refer to the exhibit.



```
FS448D-A (LAG-1) # show
config switch trunk
   edit "LAG-1"
      set mode lacp-active
      set mclag-icl enable
      set members "port13" "port14"
   next
end

FS448D-B (LAG-2) # show
config switch trunk
   edit "LAG-2"
      set mode lacp-active
      set mclag-icl enable
      set members "port13" "port14"
   next
end

FortiGate-A # show switch-controller managed-switch
config switch-controller managed-switch
   edit FS448D-A
      config ports
         edit "LAG-3"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15"
         next
      end
   next
   edit FS448D-B
      config ports
         edit "LAG-3"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15"
         next
      end
   next
end
```

Given the configuration shown in the exhibit, which two statements are true? (Choose two.)

A. LAG-3 on switches on FS448D-A and FS448D-B may be connected to a single 802.3ad trunk on another device.

B. LAG-1 and LAG-2 should be connected to a 4-port single 802.3ad trunk on another device.

C. port13 and port14 on FS448D-A should be connected to port13 and port14 on FS448D-B.

D. LAG-1 and LAG-2 should be connected to a single 4-port 802.3ad interface on the FortiGate-A.

Correct Answer: AC

QUESTION 4

A FortiGate with the default configuration shown below is deployed between two IP telephones. FortiGate receives the INVITE request shown in the exhibit from Phone A (internal) to Phone B (external).

NVITE sip:PhoneB@172.20.120.30 SIP/2.0 Via: SIP/2.0/UDP 10.31.101.20:5060 From: PhoneA To: PhoneB Call-ID: 314159@10.31.101.20 CSeq: 1 INVITE Contact: sip:PhoneA@10.31.101.20 v=0 o=PhoneA 5462346 332134 IN IP4 10.31.101.20 c=IN IP4 10.31.101.20 m=audio 49170 RTP 0 3

Which two statements are correct after the FortiGate receives the packet? (Choose two.)

A. NAT takes place only in the SIP application layer.

B. A pinhole will be opened to accept traffic sent to the FortiGate WAN IP address.

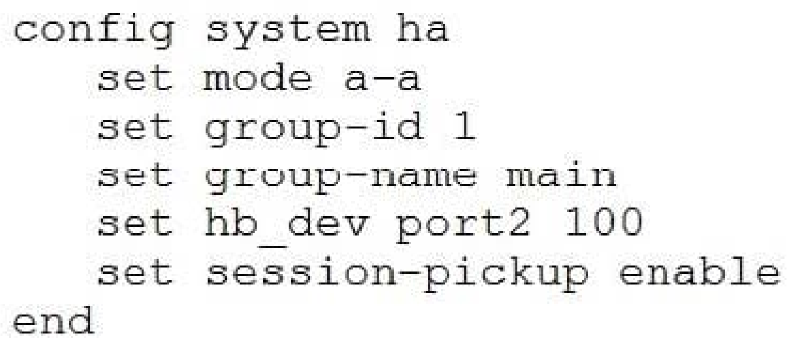
C. NAT takes place at both the network and SIP application layers.

D. A pinhole is not required to accept traffic sent to the FortiGate WAN IP address.

Correct Answer: BC

QUESTION 5

You have configured an HA cluster with two FortiGate devices. You want to make sure that you are able to manage the individual cluster members directly using port3.



```
config system ha
    set mode a-a
    set group-id 1
    set group-name main
    set hb_dev port2 100
    set session-pickup enable
end
```

Referring to the configuration shown, in which two ways can you accomplish this task? (Choose two.)

A. Create a management VDOM and disable the HA synchronization for this VDOM, assign port3 to this VDOM, then configure specific IPs for port3 on both cluster members.

B. Configure port3 to be a dedicated HA management interface; then configure specific IPs for port3 on both cluster members.

C. Allow administrative access in the HA heartbeat interfaces.

D. Disable the sync feature on port3; then configure specific IPs for port3 on both cluster members.

Correct Answer: AB