NSE8_810$^{\text{Q\&As}}$

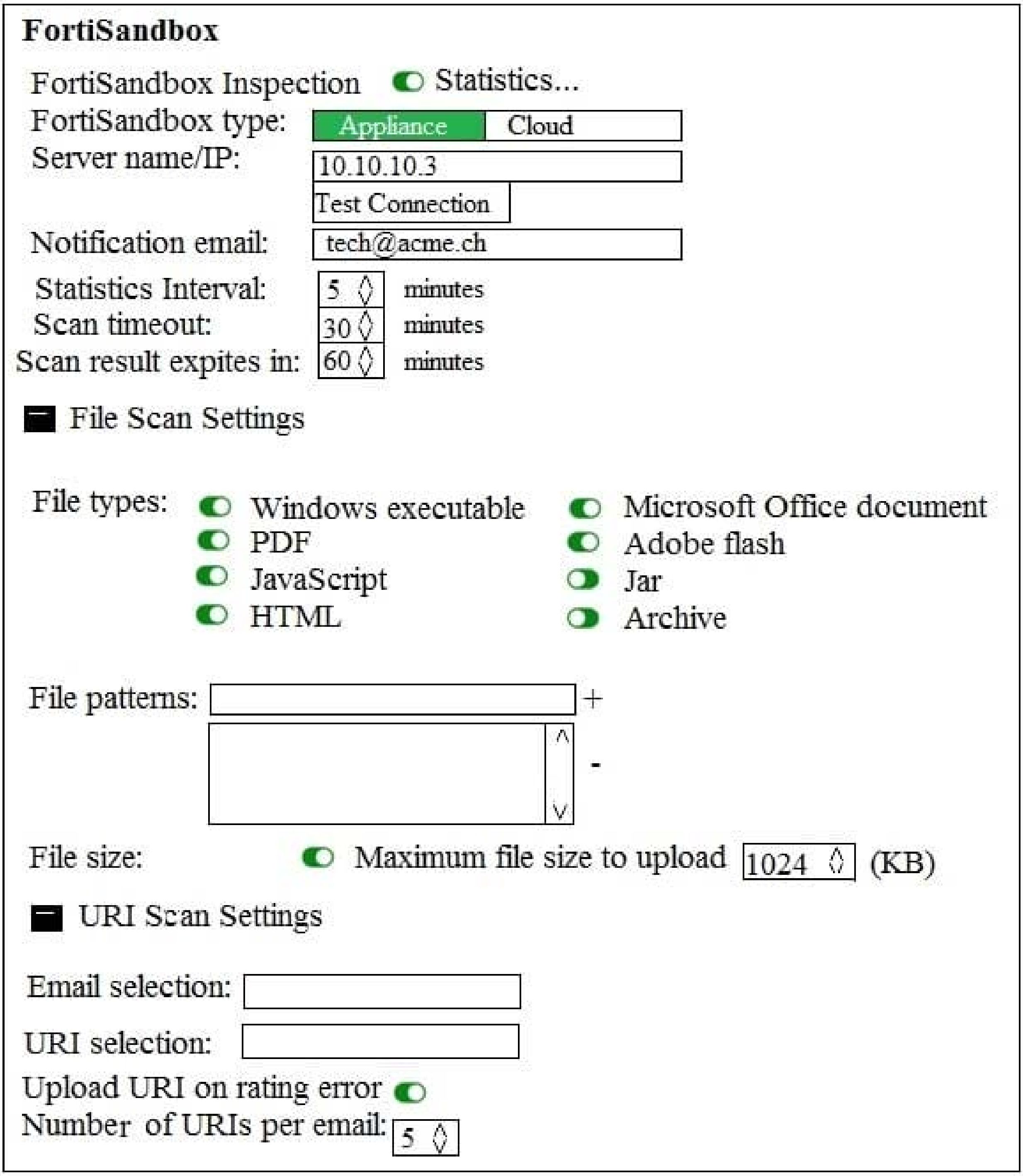
Fortinet Network Security Expert 8 Written Exam (810)

Pass Fortinet NSE8_810 Exam with 100% Guarantee

QUESTION 1

Click the Exhibit button.

You have installed a FortiSandbox and configured it in your FortiMail. Referring to the exhibit, which two statements are correct? (Choose two.)



FortiSandbox

FortiSandbox Inspection ● Statistics...

FortiSandbox type: Appliance | Cloud

Server name/IP: 10.10.10.3

Test Connection

Notification email: tech@acme.ch

Statistics Interval: 5 minutes

Scan timeout: 30 minutes

Scan result expites in: 60 minutes

File Scan Settings

File types:
- ● Windows executable
- ● PDF
- ● JavaScript
- ● HTML
- ● Microsoft Office document
- ● Adobe flash
- ○ Jar
- ○ Archive

File patterns:

File size: ● Maximum file size to upload 1024 (KB)

URI Scan Settings

Email selection:

URI selection:

Upload URI on rating error ●

Number of URIs per email: 5

A. FortiMail will cache the results for 30 minutes.

B. FortiMail will wait for 30 minutes to obtain the scan results.

C. If the FortiSandbox with IP 10.10 10 3 is not available, the e-mail will be checked by the FortiCloud Sandbox.

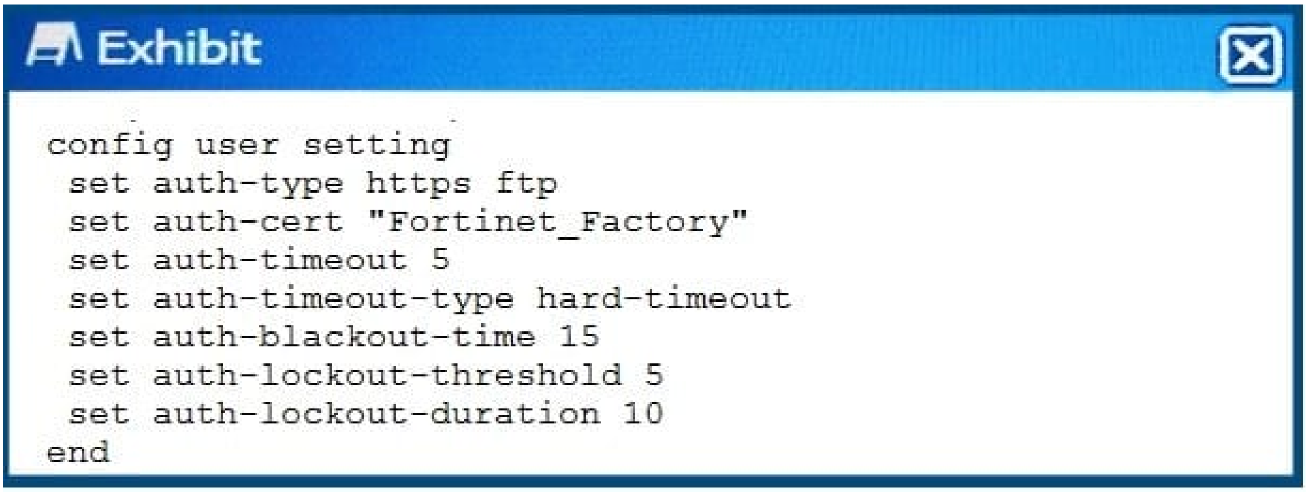
D. If FortiMail is not able to obtain the results from the fortiGuard quenes. URls will not be checked by the

FortiSandbox.

Correct Answer: BD

QUESTION 2

Click the Exhibit button.



```
config user setting
 set auth-type https ftp
 set auth-cert "Fortinet_Factory"
 set auth-timeout 5
 set auth-timeout-type hard-timeout
 set auth-blackout-time 15
 set auth-lockout-threshold 5
 set auth-lockout-duration 10
end
```

Referring to the exhibit, which two statements are true about local authentication? (Choose two.)

A. The user will be blocked 15 seconds after five login failures.

B. When a ClientHello message indicating a renegotiation is received, the FortiGate will allow the TCP connection.

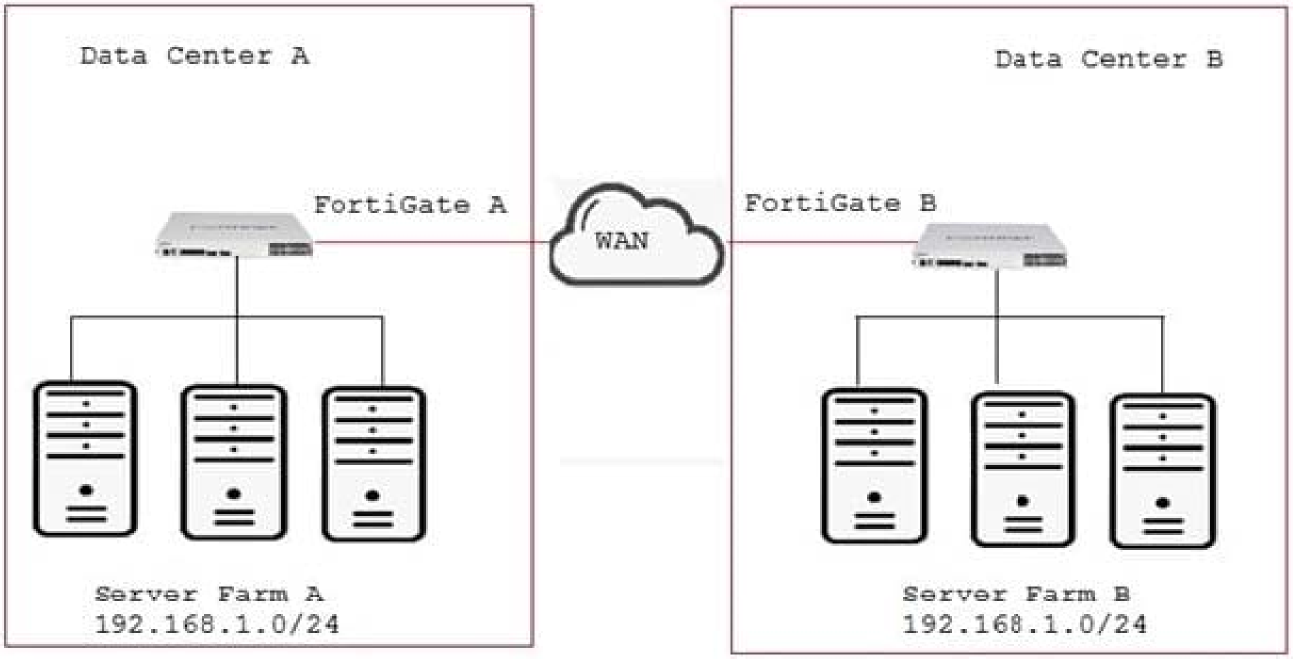
C. The user\\'s IP address will be blocked 15 seconds after five login failures.

D. After five minutes, the user will need to re-authenticate.

Correct Answer: CD

QUESTION 3

Click the Exhibit button.



Your company has two data centers (DC) connected using a Layer 3 network. Servers in farm A need to connect to servers in farm B as though they all were in the same Layer 2 segment. What would be configured on the FortiGates on each DC to allow such connectivity?

A. Create an IPsec tunnel with transport mode encapsulation.

B. Create an IPsec tunnel with Mode encapsulation.

C. Create an IPsec tunnel with VXLAN encapsulation.

D. Create an IPsec tunnel with VLAN encapsulation.

Correct Answer: C

QUESTION 4

An old router has been replaced by a FortiWAN device. The FortiWAN has inherited the router\\'s management IP address and now the network administrator needs to remove the old router from the FortiSIEM configuration.

Which two statements are true about this operation? (Choose two.)

A. FortiSIEM will discover a new device for the FortiWAN with the same IP.

B. The old router will be completely deleted from FortiSIEM\\'s CMDB.

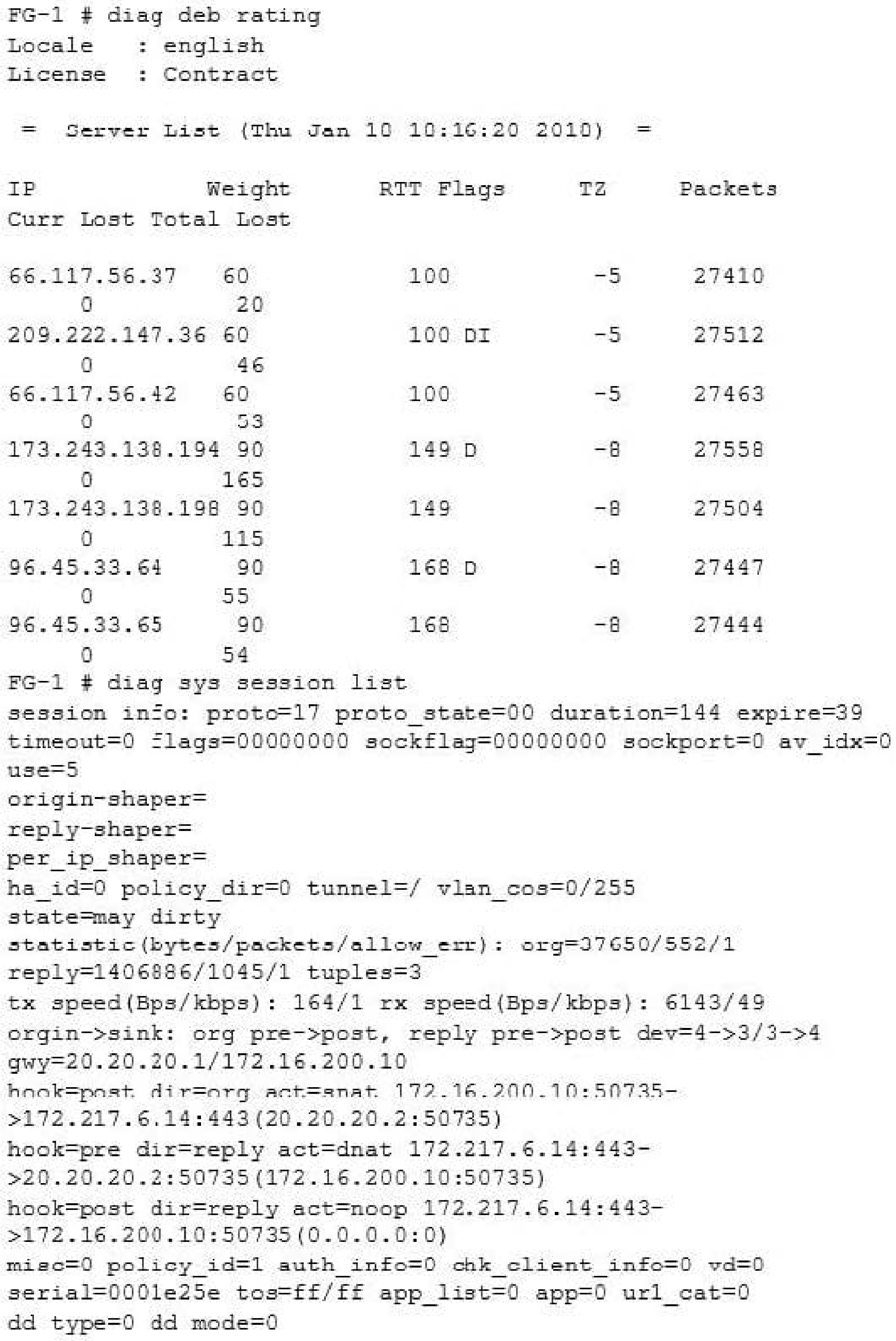
C. FotiSEIM needs a special syslog for FortiWAN.

D. FortiSIM will move the old router device into the Decommission folder.

Correct Answer: AB

QUESTION 5

Click the Exhibit button.



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

 =  Server List (Thu Jan 10 10:16:20 2010)  =

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 noticed that not all Web sessions are being inspected and you start troubleshooting the problem.

Referring to the exhibit, what would cause this problem?

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

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

C. The SSL inspection options are not set to inspection

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

Correct Answer: C

QUESTION 6

CORRECT TEXT

In a FortiGate 5000 series, two FortiControllers are working as an SLBC cluster in a-p mode. The configuration shown below is applied. config load-balance session-setup set tcp-ingress enable end When statement is true on how new TCP sessions are handled by the Distributor Processor (DP).

A. The new session added the DP session table is automatically deleted, if the traffic is denied by the processing worker.

B. No new session is added is the DP session table until the processing worker accepts the traffic.

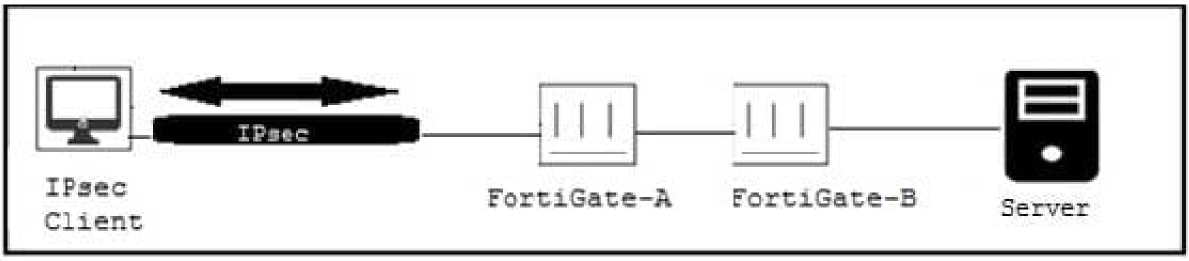
C. A new session added m the DP session table remains in the table remain in the traffic is denied by the procession worker.

D. A new session added in the OP session table remains is the table only if traffic is traffic is accepted by the processing worker.

Correct Answer: C

QUESTION 7

Click the Exhibit button.



Only users authenticated in FortiGate-B can reach the server. A customer wants to deploy a single sign-on solution for IPsec VPN users. Once a user is connected and authenticated to the VPN in FortiGate-A, the user does not need to authenticate again in FortiGate ? to reach the server.

Which two actions satisfy this requirement? (Choose two.)

A. Use Kerberos authentication.

B. FortiGate-A must generate a RADUIS accounting packets.

C. Use FortiAuthenticator.

D. Use the Collector Agent.

Correct Answer: BC

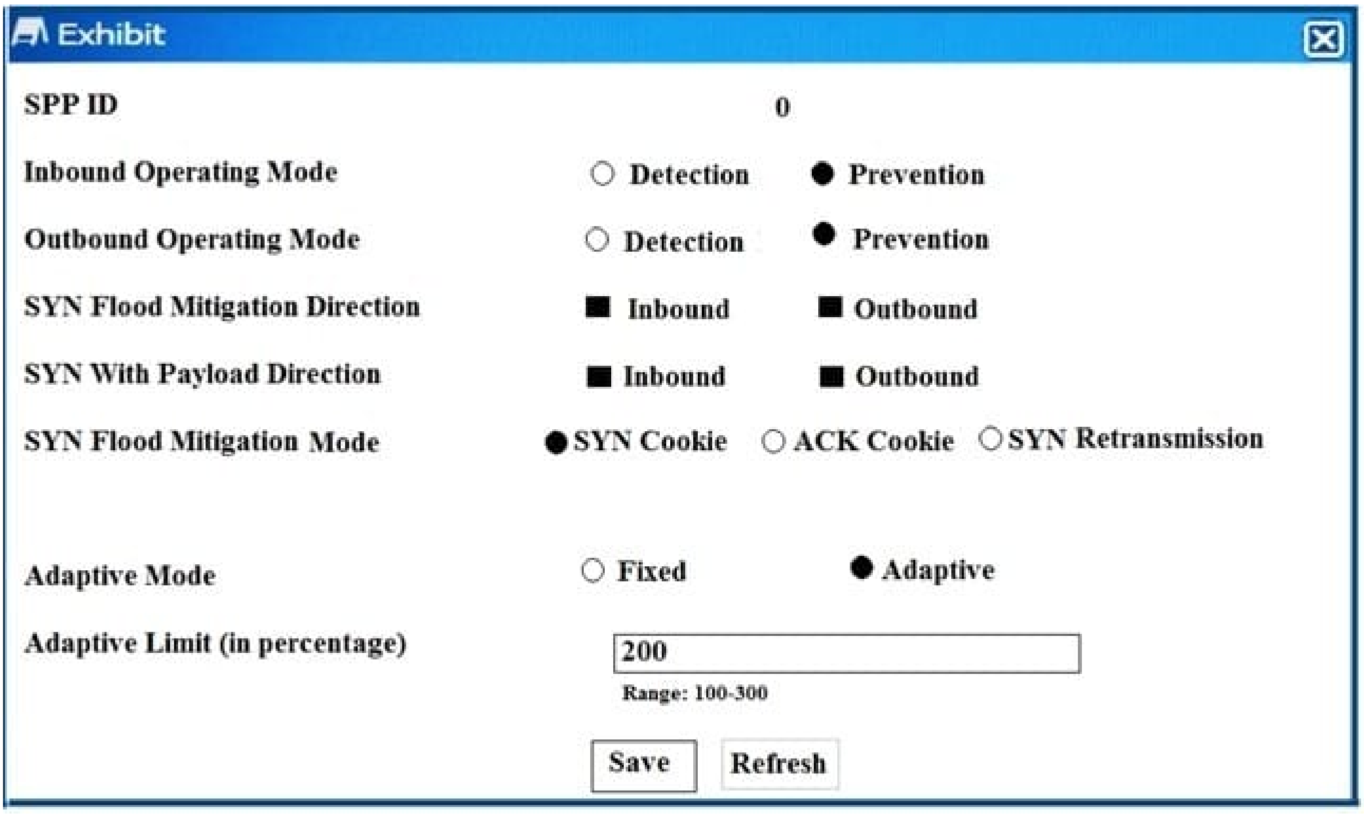
QUESTION 8

Exhibit

Click the Exhibit button.

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.)



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		

A. Traffic that does match any spp policy will not be inspection by this spp.

B. FortiDDos will not send a SYNACK if a SYN packet is coming from an IP address that is not the legtimate IP (LIP) address table.

C. FortiDooS will start dropping packets as soon as the traffic executed the configured maintain threshold.

D. SYN packets with payloads will be drooped.

Correct Answer: AB

QUESTION 9

Click the Exhibit button.

```
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
```

You have configured an HA cluster with two FortiGates. You want to make sure that you are able to

manage the individual cluster members directly using port3.

Referring to the exhibit, what are two ways to accomplish this task? (Choose two.)

A. Disable the sync feature on porl3: then configure specific IPs for ports 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. Create a management VDOM and Disable the HA synchronization for this VDOM, assign ports to this VDOM, then configure specific IPs for ports on both cluster member.

D. Allow administrative access in the HA heartbeat interfaces.

Correct Answer: BC

QUESTION 10

An organization has one central site And three remote sites. A FotiSIEM has been drafted on the central

site and now all devices across the remote sites need to be monitored by the FortiSlEM.

When action would reduce the WAN usage by the monitoring system?

A. Deploy a single Supervisor on the central site and enable WAN optimize on the WAN gateways.

B. Install local Collection remote site.

C. Disable monitoring on the remote sites during the day.

D. install a Supervisor and a Collector for each remote site.

Correct Answer: B