NSE8_810^{Q&As}

Fortinet Network Security Expert 8 Written Exam (810)

Pass Fortinet NSE8_810 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse8_810.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

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.)

![Pass2Lead](https://Pass2Lead.com)
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. URIs will not be checked by the

FortiSandbox.

Correct Answer: BD

QUESTION 2

You have a customer experiencing problem with a legacy L3L4 firewall device and IPV6 SIP VoIP traffic. They devices is dropping SIP packets, consequently, it process SIP voice calls. Which solution would solve the customer\'s problem?

A. Deploy a FortiVoice and enable IPv6 SIP.

B. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 packet.

C. Deploy a FotiVoice and enable an IPv6 SIP session helper.

D. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet

Correct Answer: D

QUESTION 3

Click the Exhibit button.

![Pass2Lead](https://Pass2Lead.com)
```
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.

![Pass2Lead](https://Pass2Lead.com)
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 4

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.)

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 5

Click the Exhibit button.
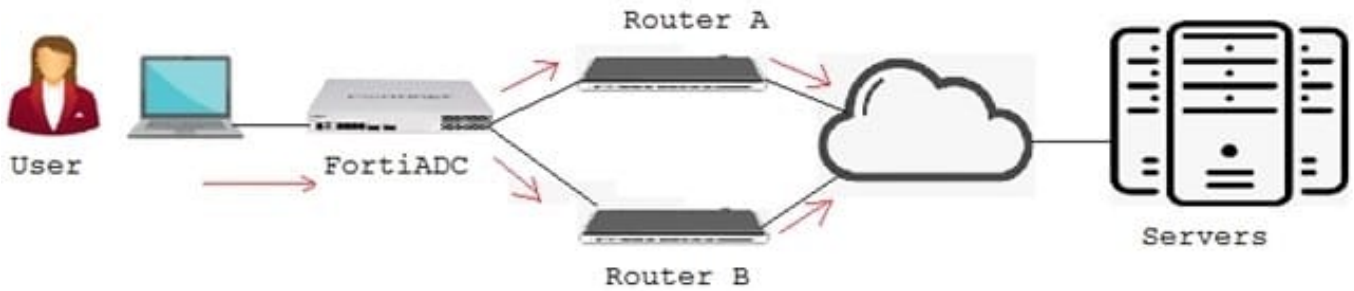
Referring to the exhibit, a FortiADC is load balancing IPv4 traffic between two next-hop routers. The FortiADC does not know the IP addresses of the servers. Also, the FortiADC is doing Layer 7 content inspection and modification.

In this scenario, which application delivery control is configured in the FortiADC?

A. Layer 2

B. Layer 3

C. Laye.4

D. Layer 7

Correct Answer: C