



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.geekcert.com/nse8_810.html

100% Passing Guarantee
100% Money Back Assurance

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

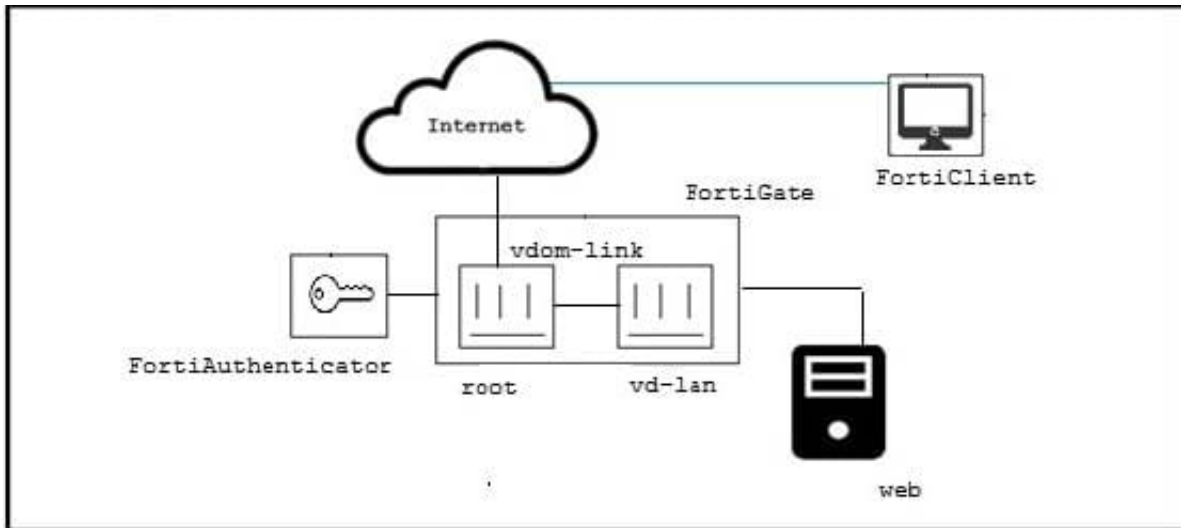
-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Exhibit The exhibit shows a topology where a FortiGate is two VDOMs, root and vd-vlan. The root VDCM provides SSL-VPN access, where the users authenticated by a FortiAuthenticator. The vd-lan VDOM provides internal access to a Web server. For the remote users to access the internal web server, there are a few requirements, which are shown below.



- At traffic must come from the SSI-VPN
- The vd-lan VDOM only allows authenticated traffic to the Web server.
- Users must only authenticate once, using the SSL-VPN portal.
- SSL-VPN uses RADIUS-based authentication.

referring to the exhibit, and the requirement describe above, which two statements are true?

(Choose two.)

- A. vd-lan authentication messages from root using FSSO.
- B. vd-lan connects to Fort authenticator as a regular FSSO client.
- C. root is configured for FSSO while vd-lan is configuration for RSSO.
- D. root sends "RADIUS Accounting Messages" to FortiAuthenticator.

Correct Answer: BD

QUESTION 2

Exhibit



```
Exhibit ✕

config antivirus profile
  edit "default"
  set comment "Scan files and block viruses."
config http
  set options scan
end
config ftp
  set options scan
end
config imap
  set options scan
end
config pop3
  set options scan
end
config smtp
  set options scan
end
config smb
  set options scan
end
  set scan-mode quick
next
end
```

Click the Exhibit button.

You are working on an entry level model FortiGate that has been configured in flow-based inspection mode with various settings optimized for performance. It appears that the main Internet firewall policy is using the antivirus profile labelled default. Your customer has found that some virus samples are not being caught by the FortiGate.

Referring to the exhibit, what is causing the problem?

- A. The set default-db configure was set to extreme.
- B. The set options scan configuration items should have been changed to not option scan avmonitor.
- C. The default AV profile was modified to use quick scan-mode.

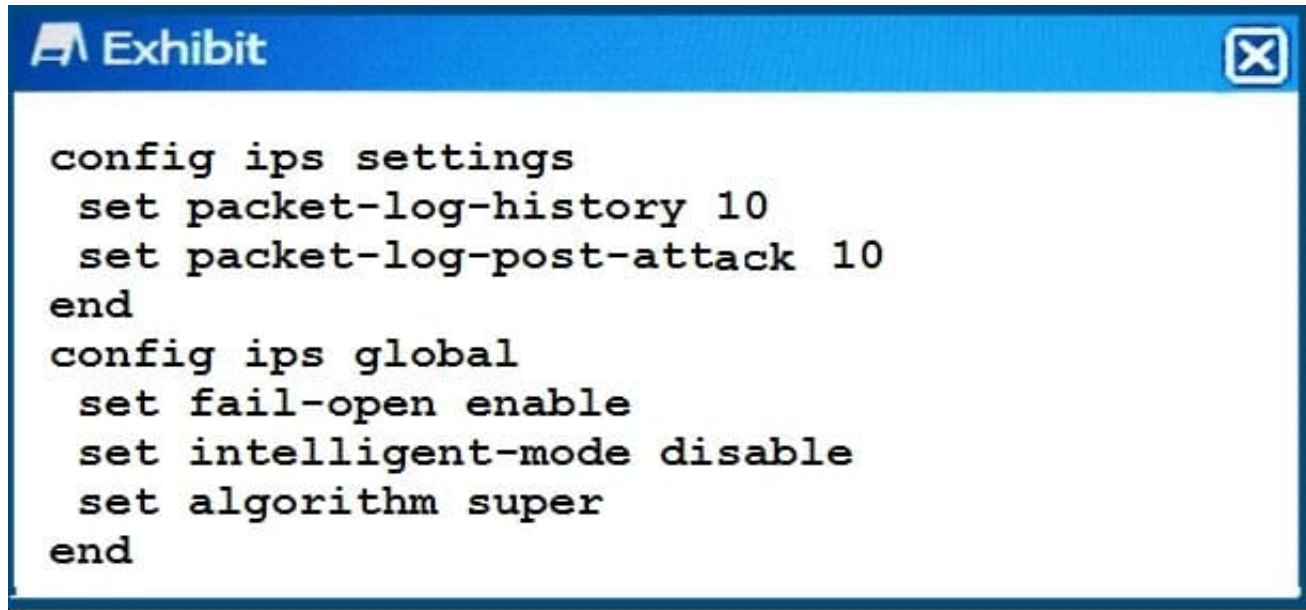


D. The mobile-malware-db configuration was set to enable.

Correct Answer: C

QUESTION 3

Exhibit An Administrator reports continuous high CPU utilization on a FortiGate device due to the IPS engine. The exhibit shows the global IPS configuration. Which two configuration actions will reduce the CPU usage? (Choose two.)



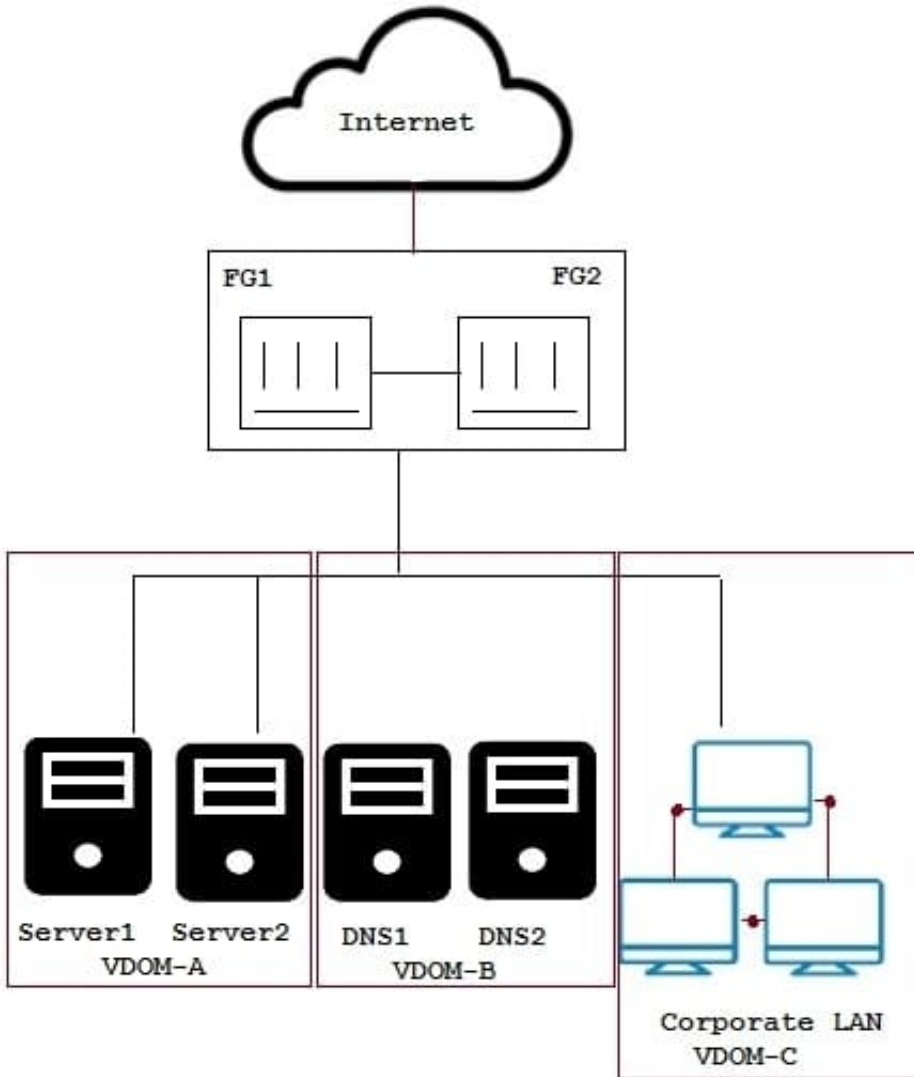
```
config ips settings
  set packet-log-history 10
  set packet-log-post-attack 10
end
config ips global
  set fail-open enable
  set intelligent-mode disable
  set algorithm super
end
```

- A. Disable fail open.
- B. Enable intelligent mode.
- C. Change the algorithm to low.
- D. Reduce the number of packets logged.

Correct Answer: CD

QUESTION 4

Click to the Exhibit button. You need to apply the security features below to the network shown in the exhibit. -high grade DDoS protection -Web security and load balancing for Server1 and Server2 -Solution must be PCI DSS compliant -Enhanced security to DNS 1 and DNS 2



What are three solutions for this scenario? (Choose three.)

- A. FortiWeb for VDOM-A
- B. FortiDDoS between FG1 and FG2 and the Internet
- C. FortiADC for VDOM-A
- D. FortiADC for VDOM-B
- E. FortiDDoS between FG1 and FG2 and VDOMs

Correct Answer: CDE

QUESTION 5

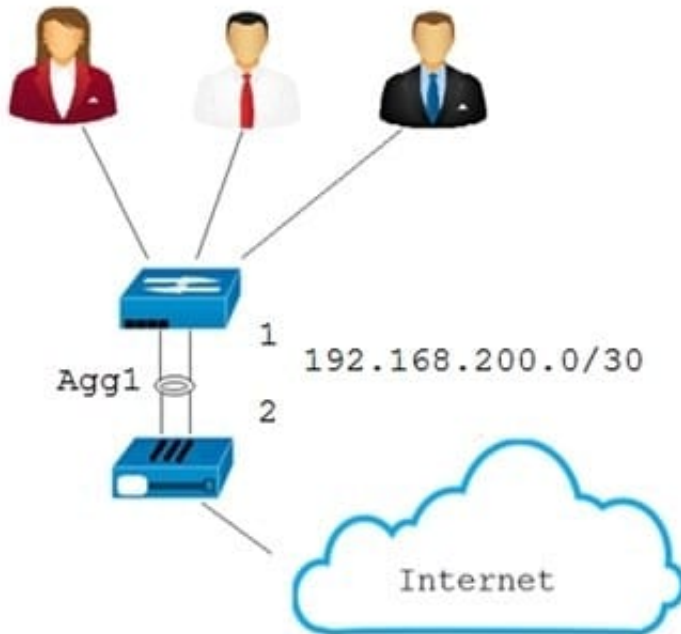
Click the exhibit.

You created an aggregate interface between your FortiGate and a switch consisting of two 1 Gbps links as shown in the



exhibit. However, the maximum bandwidth never exceeds 1 Gbps and employees are complaining that the network is slow. After troubleshooting, you notice only one member interface is being used. The configuration for the aggregate interface is shown in the exhibit.

In this scenario, which command will solve this problem?



```
config system interface
edit "Agg1"
set ip 192.168.200.2 255.255.255.252
set type aggregate
set member port1 port2
set vdom "root"
set weight 1
set lacp-mode passive
set min-links 1
set algorithm L2
next
end
```

- A. config system interface edit Agg1 set min-links 2 end
- B. config system interface edit Agg1 set weight 2 end
- C. config system interface edit Agg1 set Algorithm L4 end
- D. config system interface edit Agg1 set lacp-mode active end

Correct Answer: A