NSE8_811 Q&As

Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

https://www.geekcert.com/nse8_811.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Consider the following FortiGate configuration: Which command-line option for deep inspection SSL would have the FortiGate re-sign all untrusted self-signed certificates with the trusted Fortinet_CA_SSL certificate?

```
config firewall ssl-ssh-profile
    edit "custom-deep-inspection"
        config https
            set untrusted-cert {option}
        end
    next
end
```

A. block

B. inspect

C. allow

D. ignore

Correct Answer: D

QUESTION 2

Refer to the exhibit.

```
config waf url-rewrite url-rewrite-rule
    edit "NSE8-rule"
        set action redirect
        set location "https://$0/$1"
        set host-status disable
        set host-use-pserver disable
        set referer-status disable
        set referer-use-pserver disable
        set url-status disable
config match-condition
    edit 1
        set reg-exp "(.*)"
        set protocol-filter enable
    next
    edit 2
        set object http-url
        set reg-exp "^/(.*)$"
    next
end
    next
end
config waf url-rewrite url-rewrite-policy
    edit "nse8-rewrite"
config rule
    edit 1
        set url-rewrite-rule-name "NSE8-rule"
    next
    end
    next
end
```

The exhibit shows the steps for creating a URL rewrite policy on a FortiWeb. Which statement represents the purpose of this policy?

A. The policy redirects all HTTPS URLs to HTTP.

B. The policy redirects all HTTP URLs to HTTPS.

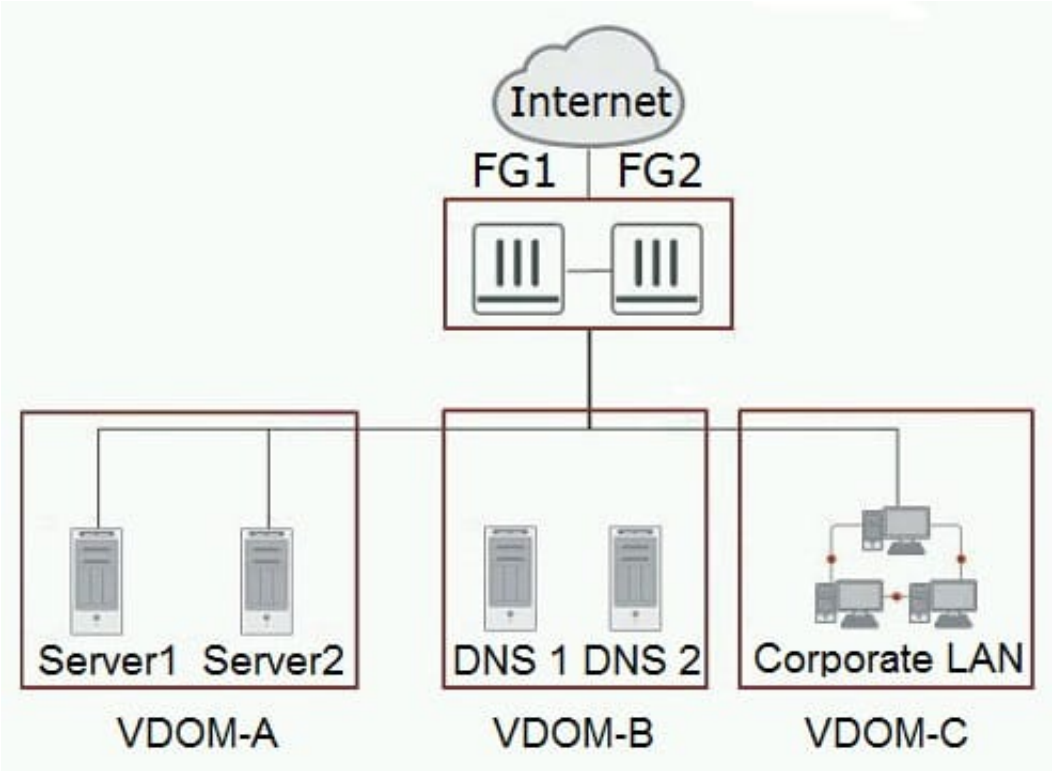
C. The policy redirects only HTTP URLs containing the ^/(.*)$ string to HTTPS.

D. The policy redirects only HTTPS URLs containing the ^/(.*)$ string to HTTP.

Correct Answer: B

QUESTION 3

Refer to the exhibit.



You need to apply the security features listed below to the network shown in the exhibit.

High grade DDoS protection Web security and load balancing for Server 1 and Server 2 Solution must be PCI DSS compliant Enhanced security to DNS 1 and DNS 2

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

A. FortiDDoS between FG1 and FG2 and the Internet

B. FortiADC for VDOM-A

C. FortiWeb for VDOM-A

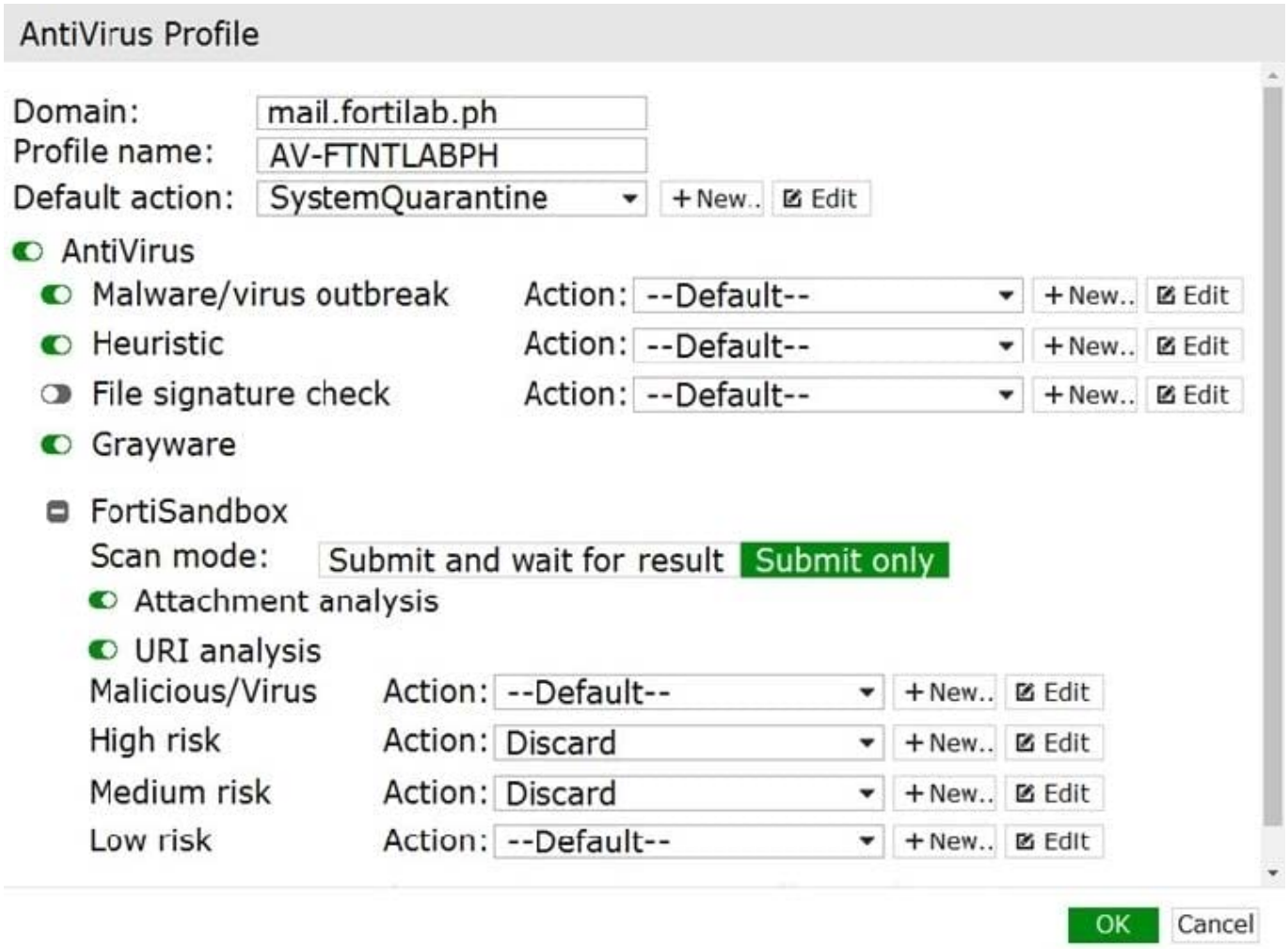
D. FortiADC for VDOM-B

E. FortiDDoS between FG1 and FG2 and VDOMs

Correct Answer: ACD

QUESTION 4

Refer to the exhibit.



Referring to the exhibit, what will happen if FortiSandbox categorizes an e-mail attachment submitted by FortiMail as a high risk?

A. The high-risk file will be discarded by attachment analysis.

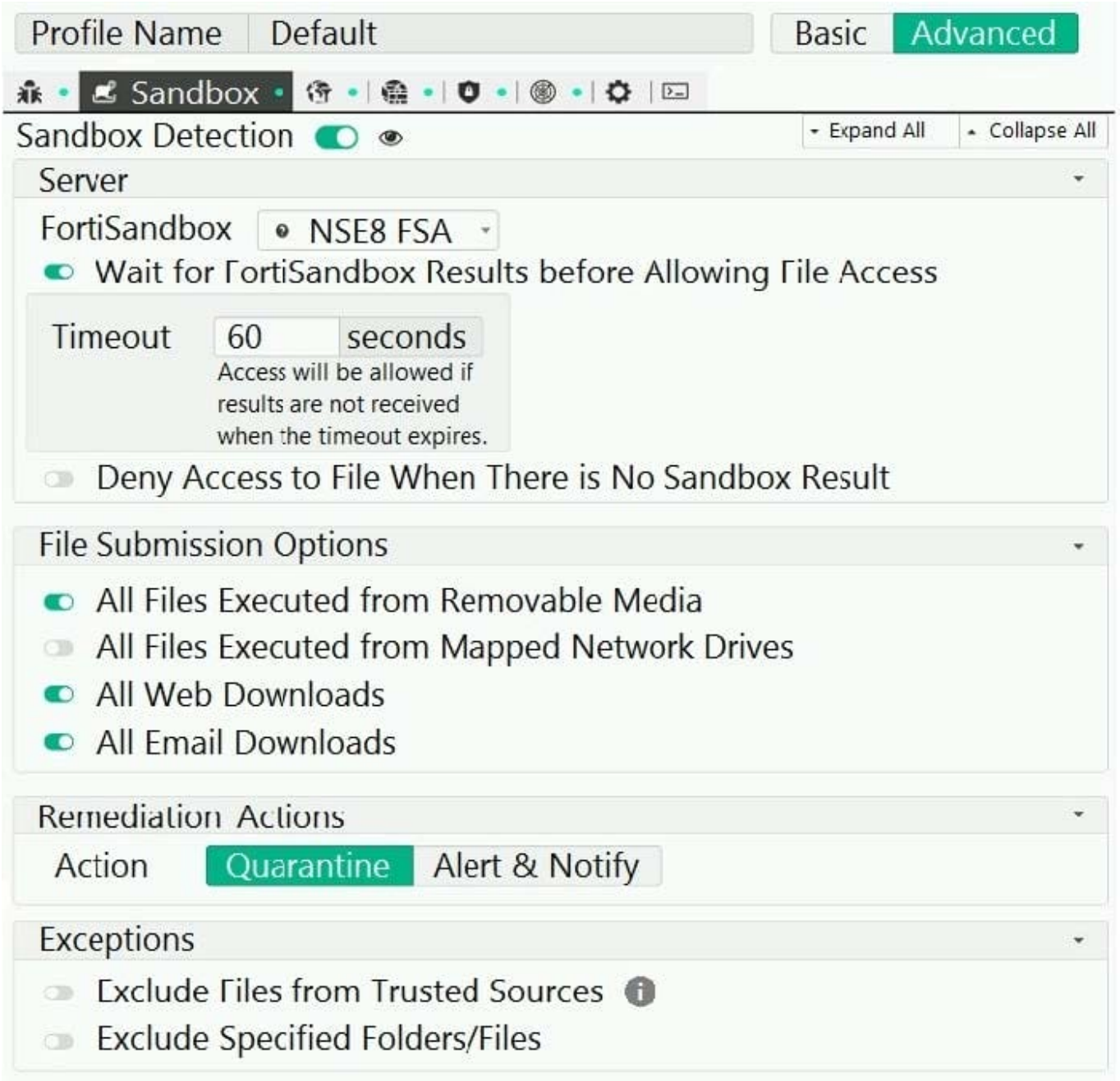
B. The high-risk file will go to the system quarantine.

C. The high-risk file will be received by the recipient.

D. The high-risk file will be discarded by malware/virus outbreak protection.

Correct Answer: D

QUESTION 5



Anti-Virus Real-Time Protection is enabled without any exclusions.

Referring to the exhibit, which two behaviors will the FortiClient endpoint have after receiving the profile update from the FortiClient EMS? (Choose two.)

A. Access to a downloaded file will always be allowed after 60 seconds when the FortiSandbox is reachable.

B. The user will not be able to access a downloaded file for a maximum of 60 seconds if it is not a virus and the FortiSandbox is reachable.

C. Files executed from a mapped network drive will not be inspected by the FortiClient endpoint AntiVirus engine.

D. If the Real-Time Protection does not detect a virus, the user will be able to access a downloaded file when the FortiSandbox is unreachable.

Correct Answer: AB