



FORTISANDBOX^{Q&As}

FortiSandbox 2.0.3 Specialist

Pass Fortinet FORTISANDBOX Exam with 100% Guarantee

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

<https://www.pass4itsure.com/fortisandbox.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

When does a FortiSandbox categorize a file as suspicious?

- A. When the file is detected as known greyware
- B. When the file matches an antivirus signature that might detect false positives
- C. When the file matches a signature in the extended antivirus database
- D. When the file is not detected as a known malware, but it has some of the same behaviors as malware

Correct Answer: D

QUESTION 2

Which FortiGate process sends files to FortiSandbox for inspection?

- A. scanunit
- B. fortisandboxd
- C. miglogd
- D. quarantine

Correct Answer: A

QUESTION 3

Based on the exhibit, which files will be sent to FortiSandbox? (Choose three.)



```
config antivirus profile
  edit "default"
    set comment "Scan filter and block viruses."
    set ftgd-analytics everything
    set analytics-max-upload 13
    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
  next
end
config firewall profile-protocol-options
  edit "default"
    set comment "All default services."
    config http
      set ports 80
      unset options
      unset post-long
      set oversize-limit 20
      set uncompressed-oversize-limit 15
      set uncompressed-nest limit 5
    end
    config ftp
      set ports 21
      set status disable
      set options splice
      set oversize-limit 50
    end
    config imap
      set ports 143
      set options fragmail
    end
    config mapi
      set ports 135
      set options fragmail
    end
    config pop3
      set ports 110
      set options fragmail
    end
    config smtp
      set ports 25
      set options fragmail splice
    end
    config nntp
      set ports 119
      set options splice
    end
    config dns
      set ports 53
    end
  next
end
```

- A. A 7 MB PDF attachment to an email, sent over SMTP.
- B. A 3 MB archive that decompresses to 16 MB, sent over HTTP.



- C. A 3 MB Flash video, sent over HTTP.
- D. An 11 MB EXE file, sent of HTTP, detected as suspicious.
- E. A 5 MB EXE file attached to an email, sent over POP3, detected as known malware.

Correct Answer: ACD

QUESTION 4

On FortiMail which type of profile is used to configure when files are sent to a FortiSandbox?

- A. Content profile
- B. Antivirus profile
- C. Protocol options profile
- D. Antispam profile

Correct Answer: B

QUESTION 5

FortiGate is configured to send suspicious files to a FortiSandbox for in-line inspection. The administrator creates a new VDOM, and then generates some traffic so what the new VDOM sends a file to the FortiSandbox for the first time.

Which is true regarding this scenario?

- A. FortiSandbox will store the file, but not inspect it until the administrator manually authorizes the new VDOM.
- B. Before generating traffic, the administrator can push the VDOM configuration from the FortiGate to the FortiSandbox. Then when FortiSandbox receives the file, FortiSandbox will inspect the file.
- C. FortiSandbox can be pre-configured to automatically authorize the new VDOM and inspect the file.
- D. FortiSandbox will store the file, but not inspect it until the administrator manually adds the new VDOM to the FortiSandbox configuration.

Correct Answer: B

[Latest FORTISANDBOX Dumps](#)

[FORTISANDBOX VCE Dumps](#)

[FORTISANDBOX Study Guide](#)