Vendor: Fortinet

Exam Code:FORTISANDBOX

Exam Name: FortiSandbox 2.0.3 Specialist

Version: Demo

QUESTION 1

What is the minimum FortiAnalyzer firmware version that supports FortiSandbox device registration?

A. 5.0.6

B. 5.0.11

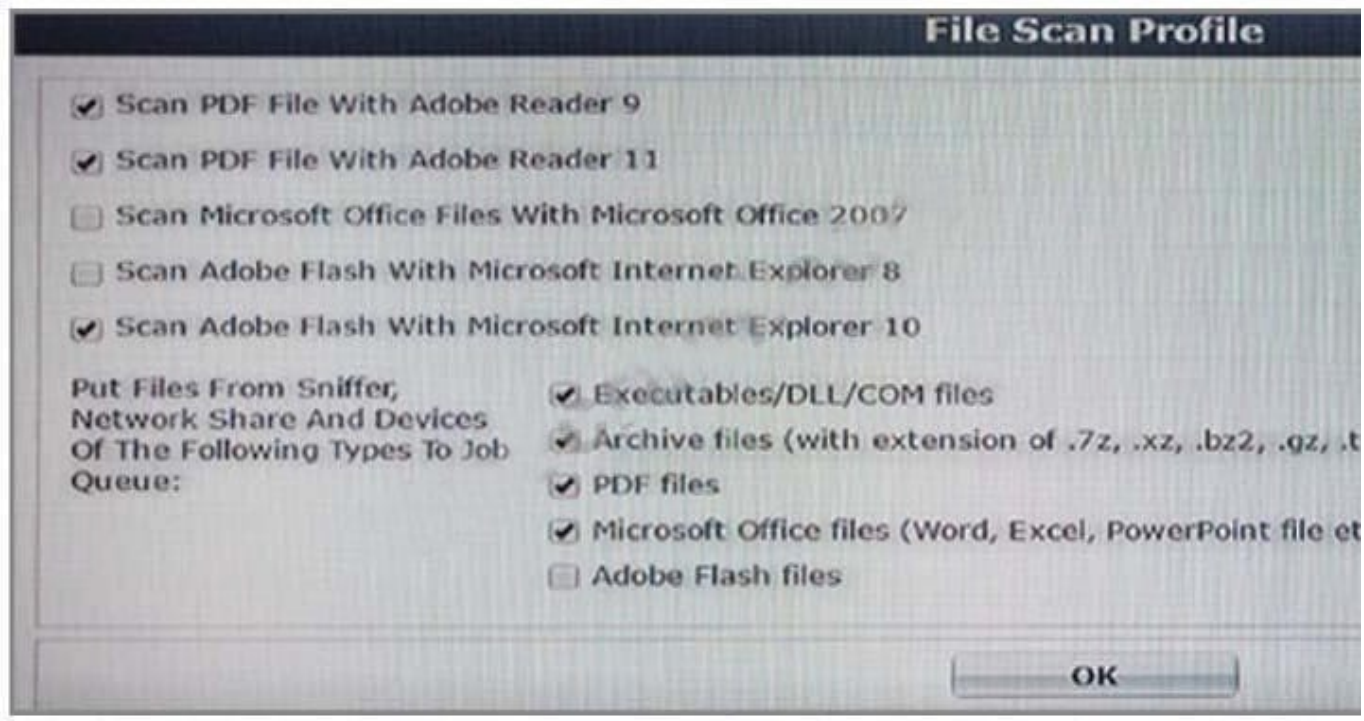
C. 5.0.8

D. 5.2.1

Correct Answer: C

QUESTION 2

Based on the exhibit, which are true? (Choose two.)



A. Depending on the version indicated in the PDF file, FortiSandbox will scan using only one PDF reader (either Adobe Reader 9 or Adobe Reader 11).

B. If there are no Internet Explorer 10 installations in your network, you can safely disable the scanning of Adobe Flash with Microsoft Internet Explorer 10.

C. FortiSandbox will scan all Flash applications using Internet Explorer 10. This does not guarantee safety for Internet Explorer 8.

D. You can safely disable the PDF scanning with Acrobat Reader 9 because PDF scanning with Acrobat Reader 11 is enabled.

Correct Answer: AC

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

What mechanism does FortiGate use to avoid sending a file that has been already inspected to FortiSandbox?

A. FortiGate sends the file name to FortiGuard. FortiGuard checks if a file with that name has been already inspected.

B. FortiGate sends the file name to FortiSandbox. FortiSandbox checks if it has already inspected a file with that name.

C. FortiGate sends a hash of the file to FortiSandbox. FortiSandbox checks if it has already inspected a file with that hash.

D. FortiGate searches its cache of a list of file names that it has already inspected.

Correct Answer: B

QUESTION 5

You can configure FortiGate and FortiMail to send potentially malicious files to FortiSandbox. Which file types are considered to be potentially malicious? (Choose three.)

A. JPEG images

B. Rich text format (RTF)

C. Adobe PDF

D. Adobe Flash

E. Microsoft PowerPoint

Correct Answer: CDE

QUESTION 6

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 7

Which protocols can a FortiSandbox inspect when is deployed in sniffer mode? (Choose two.)

A. MAPI

B. FTPS

C. HTTP

D. POP3

Correct Answer: CD

QUESTION 8

Which methods can be used to submit files to FortiSandbox for inspection? (Choose two.)

A. File shares

B. FTP upload

C. SFTP upload

D. JSON API

Correct Answer: AD

QUESTION 9

Which devices can be configured to send files to FortiSandbox 2.0.3? (Choose two.)

A. FortiGate

B. FortiMail

C. FortiSwitch

D. FortiAP

Correct Answer: AB

QUESTION 10

Which are true about activating the Microsoft Office license in a FortiSandbox? (Choose two.)

A. Happens simultaneously with the activation of the Windows licenses

B. Does not require Internet access

C. Requires that you download a license file from the Fortinet support website

D. Requires you to enter the key in the FortiSandbox GUI

Correct Answer: CD

QUESTION 11

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

QUESTION 12

The Windows licenses in a FortiSandbox could be locked because they have exceeded the maximum

number of allowed activations.

What should the administrator do to fix the problem?

A. Contact Microsoft support.

B. Restore a backup of the configuration taken before the licenses became locked.

C. Reinstall the license files.

D. Contact Fortinet support.

Correct Answer: D