**Vendor:**Fortinet

**Exam Code:**FORTISANDBOX

**Exam Name:**FortiSandbox 2.0.3 Specialist

**Version:**Demo

**QUESTION 1**

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 2**

If FortiSandbox connects to FortiGuard through a web proxy server, which FortiSandbox interface must have access to the proxy server?

A. port3

B. port2

C. port1

D. port4

Correct Answer: C

---

**QUESTION 3**

Which threats can a FortiSandbox inspect when it is deployed in sniffer mode? (Choose three.)

A. Suspicious website access

B. Botnet connections

C. Applications that use excessive bandwidth

D. Known viruses

E. Spam

Correct Answer: ABE

---

**QUESTION 4**

Which FortiGate process sends files to FortiSandbox for inspection?

A. scanunit

B. fortisandboxd

C. miglogd

D. quarantine

Correct Answer: A

---

**QUESTION 5**

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 6**

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 7**

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 8**

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 9**

Which browser is installed in the Windows 7 x86 VM image?

A. Internet Explorer 9

B. Firefox

C. Google Chrome

D. Internet Explorer 10

Correct Answer: A

---

**QUESTION 10**

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 11**

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 12**

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