FortiSandbox.VCEplus.premium.exam.15q

Number: FortiSandbox
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

FortiSandbox 2.0.3 Specialist

Version 1.0

Exam A

QUESTION 1 Which threats can a FortiSandbox inspect when it is deployed in sniffer mode?
(Choose three.)

A. Applications that use excessive bandwidth
B. Suspicious website access
C. Spam
D. Botnet connectionsE. Known viruses

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

Which is true regarding Microsoft Office on FortiSandbox?

A. Office 365 files are not supported.
B. Microsoft Office is not included. You must purchase it separately, then manually install it in the applicable VMs on FortiSandbox.
C. Office 2013 is installed in one of the VMs.
D. Microsoft Word documents (.docx) are not inspected.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

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
Section: (none)
Explanation

Explanation/Reference:
Reference: http://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%20Input/600_Device/200_Supported%20Devices/100_Supported%20Devices.htm

QUESTION 4 Which methods can be used to submit files to FortiSandbox for inspection?
(Choose two.)

A. File shares
B. SFTP upload
C. FTP upload
D. JSON API

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 Which protocols can FortiSandbox use to connect to a network file share? (Choose two.)

A. HTTP
B. NTFSv2
C. CIFS
D. FTP

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
If FortiSandbox connects to FortiGuard through a web proxy server, which FortiSandbox interface must have access to the proxy server?

A. port4
B. port1
C. port3
D. port2

Correct Answer:
B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 Which protocols can a FortiSandbox inspect when is deployed in sniffer mode? (Choose two.)

A. FTPS
B. POP3
C. MAPI
D. HTTP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 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
Section: (none)
Explanation

Explanation/Reference:
Reference: http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-sandbox-inspection-54/1-sandbox-introduction/3-Sending-files.htm

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

```
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
```

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

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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 Fortinet support
B. Contact Microsoft support
C. Reinstall the license files
D. Restore a backup of the configuration taken before the licenses became locked

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 Which protocols are supported for archiving scan job reports? (Choose two.)

A. CIFS
B. NFSv2
C. SMB
D. FTP

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference: