

NSE7_ATP-2.5.vceplus.premium.exam.30q

Number: NSE7_ATP-2.5

Passing Score: 800

Time Limit: 120 min

File Version: 1.0



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

NSE7_ATP-2.5

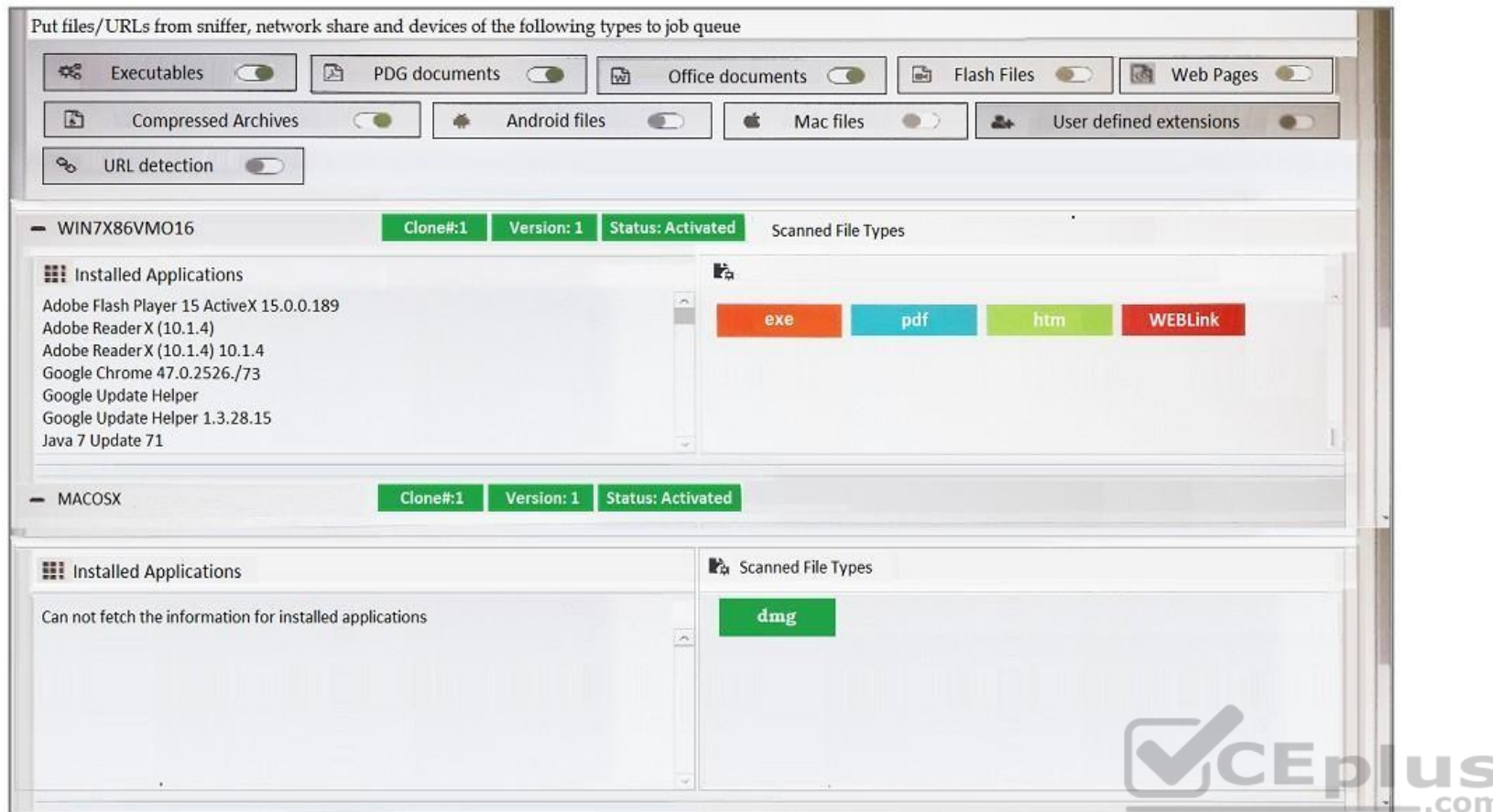
Fortinet NSE 7 - Advanced Threat Protection 2.5



Exam A

QUESTION 1

Examine the FortiSandbox **Scan Profile** configuration shown in the exhibit, and then answer the following question:



Based on the configuration, which of the following statements are true? (Choose two.)

- A. PDF files will be inspected in the **WIN7X86VM)16** VM.
- B. URLs submitted using JSON API will not be inspected.
- C. HTM files submitted using the management GUI will be inspected.
- D. DMG files will be inspected in the **MACOSX** VM.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2 Which samples can FortiClient submit to FortiSandbox for analysis?

(Choose two.)

- A. Downloads from emails
- B. URLs from web requests
- C. Command and control traffic
- D. Files from removable storage

Correct Answer: AC




Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Examine the FortiGate antivirus logs shown in the exhibit, then answer the following question:

<div>   <input type="button" value="Add Filter"/> <div>  <input type="button" value="Details"/> </div> </div>									
#		Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
1		02-12 11:38	HTTP	10.0.1.10	fsa_dropper.exe	FSA/RISK_HIGH		host: 100.64.1.10	blocked
2		02-12 11:34	HTTP	10.0.1.10	fsa_downloader.exe	low risk		host: 100.64.1.10	monitored
3		02-12 11:30	HTTP	10.0.1.10	fsa_downloader.exe			host: 100.64.1.10	analytics
4		02-12 11:04	HTTP	10.0.1.10	fsa_sample_1.exe	clean		host: 100.64.1.10	monitored
5		02-12 11:00	HTTP	10.0.1.10	fsa_sample_1.exe			host: 100.64.1.10	analytics
6		02-12 11:00	HTTP	10.0.1.10	eicar.exe	EICAR_TEST_FILE		host: 100.64.1.10	blocked

Based on the logs shown, which of the following statements is correct? (Choose two.)

- A. The `fsa_dropper.exe` file was blocked using a local black list entry.
- B. The `fsa_sample_1.exe` file was not sent to FortiSandbox.
- C. The `eicar.exe` file was blocked using a FortiGuard generated signature.
- D. The `fsa_downloader.exe` file was not blocked by FortiGate.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

File Filter allows the Web Filter profile to block files passing through a FortiGate based on file type. Reference:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/610893/file-filter>

QUESTION 4

At which stage of the kill chain will an attacker use tools, such as nmap, ARIN, and banner grabbing, on the targeted organization's network?

- A. Exploitation
- B. Reconnaissance
- C. Lateral movement
- D. Weaponization

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

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

Which of the following is true regarding this scenario?

- A. FortiSandbox will accept the file, but not inspect it until the administrator manually configures the new VDOM on FortiSandbox.
- B. FortiSandbox will inspect all files based on the root VDOM authorization state and configuration.
- C. FortiSandbox will accept the file, but not inspect it until the administrator manually authorizes the new VDOM on FortiSandbox.

D. By default, FortiSandbox will autoauthorize the new VDOM, and inspect files as they are received.

Correct Answer: B






Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Examine the System Information widget shown in the exhibit, then answer the following question:

System Information	
Unit Type	Standalone
Host Name	FSAVM0I000009553 [Change]
Serial Number	FSAVM0I000009553
System Time	Fri Dec 1 16:35:52 2017 UTC [Change]
Firmware Version	v2.5.0,build0322 (Interim) [Update]
VM License	 [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 10 hour(s) 4 minute(s)
Windows VM	
Microsoft Office	 [Upload License]
VM Internet Access	 [(SIMNET ON)]
FDN Download Server	

Which of the following inspections will FortiSandbox perform on samples submitted for sandboxing? (Choose two.)

- A. URL rating on FQDN seen in DNS requests
- B. IP reputation check on callback connections
- C. Antivirus inspection on downloaded files
- D. URL rating on HTTP GET requests

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7 Which of the kill chain stages does Fortinet's advanced threat protection solution block?
(Choose three.)

- A. Command and control
- B. Delivery
- C. Reconnaissance
- D. Lateral movement
- E. Weaponization

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8 Which of the following are features of network share scanning of FortiSandbox?
(Choose two.)

- A. Move clean files to a separate network share.
- B. Replace suspicious files with a replacement message.
- C. Detect malicious URLs.
- D. Detect network attacks.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference: https://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%20Input/900_Network%20Share/100_Network%20Share.htm

QUESTION 9 When using FortiSandbox in sniffer-mode, you should configure FortiSandbox to inspect both inbound and outbound traffic.

What type of threats can FortiSandbox detect on inbound traffic? (Choose two.)

- A. Botnet connections
- B. Malware
- C. Malicious URLs
- D. Intrusion attempts

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Which of the advanced threat protection solutions should you use to protect against an attacker may take during the lateral movement stage of the kill chain? (Choose two.)

- A. FortiClient and FortiSandbox
- B. FortiMail and FortiSandbox
- C. FortiGate and FortiSandbox
- D. FortiWeb and FortiSandbox

Correct Answer: BD

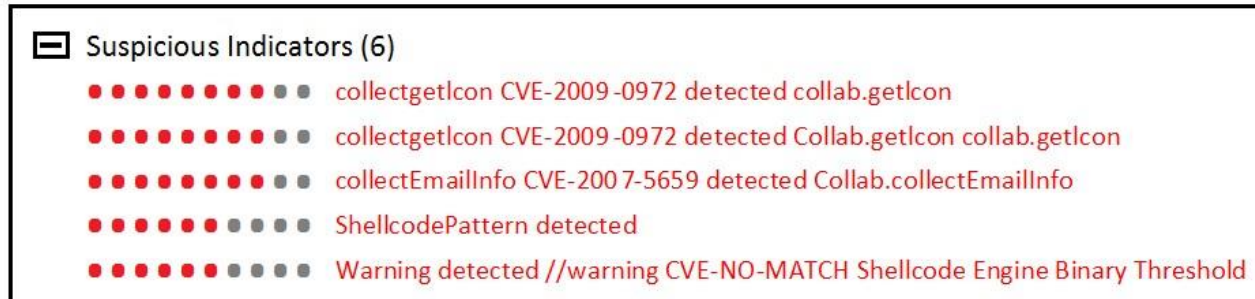
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Examine the Suspicious Indicators section of the scan job shown in the exhibit, then answer the following question:



Which FortiSandbox component identified the vulnerability exploits?

- A. VM scan
- B. Antivirus scan
- C. Static analysis
- D. Cache check

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 12

Which advanced threat protection integration solution should you use to protect against out-of-band attack vectors, such as USB drives, used during the delivery stage of the kill chain?

- A. FortiGate and FortiSandbox
- B. FortiMail and FortiSandbox
- C. FortiWeb and FortiSandbox
- D. FortiClient and FortiSandbox

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.infosecpartners.com/fortimail-fortisandbox-perfect-partners/>

QUESTION 13 Which of the following advanced threat protection are capable of preventing patient-zero infections?

(Choose two.)

- A. FortiWeb and FortiSandbox
- B. FortiClient and FortiSandbox
- C. FortiMail and FortiSandbox
- D. FortiGate and FortiSandbox

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

FortiGate Enterprise Firewall Platform provides the industry's highest- performing firewall capabilities, and Fortinet's FortiGuard Security Subscription Services provide the industry's highest level of threat research, intelligence, and analytics.

Reference: <https://www.fortinet.com/content/dam/fortinet/assets/alliances/2019/sb-fortinet-alliances-ziften.pdf>

QUESTION 14 Which of the following scan job report sections are generated by static analysis? (Choose two.)

- A. Office Behaviors
- B. Launched Processes
- C. Registry Changes
- D. Virtual Simulator

Correct Answer: CD

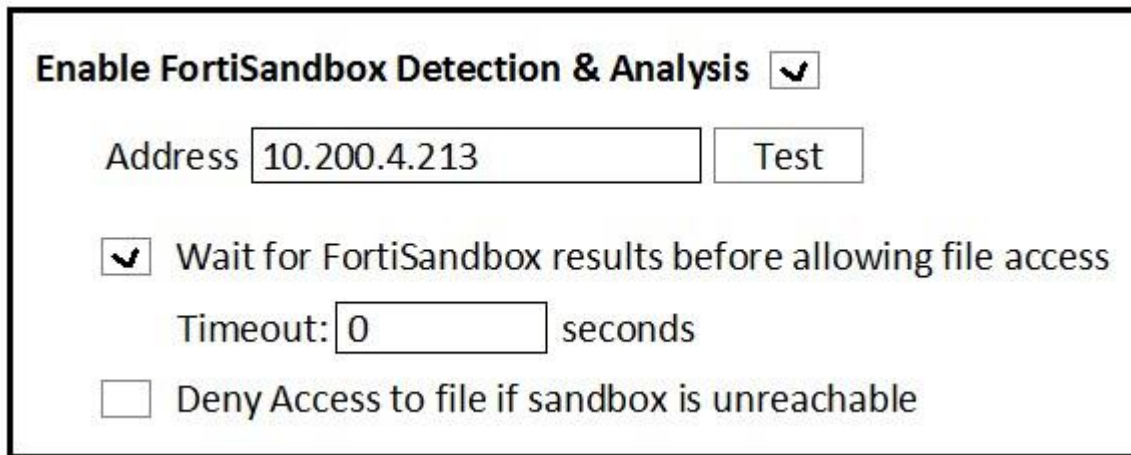
Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Examine the FortiClient configuration shown in the exhibit. then answer the following question:



What is the general rule you should follow when configuring the **Timeout** value for files submitted to FortiSandbox?

- A. It should be long enough for FortiSandbox to complete an antivirus scan of files.
- B. It should be long enough for FortiSandbox to complete a cloud query of file hashes.
- C. It should be long enough for FortiSandbox to complete sandbox analysis of files.
- D. It should be long enough for FortiSandbox to complete a static analysis of files.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference https://help.fortinet.com/fclient/olh/5-6-6/FortiClient-5.6-Admin/800_Sandbox%20Detection/0605_Config%20submission%20and%20remediation.htm

QUESTION 16 FortiSandbox generates structured threat information exchange (STIX) packages for which of the following threats? (Choose two.)

- A. Botnet connections

- B. Malware
- C. Intrusion attempts
- D. Malicious URLs

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortisandbox/3.0.3/administration-guide/170699/ioc-package>

QUESTION 17 Which FortiSandbox interfaces can you use for sniffer mode? (Choose two.)

- A. port2
- B. port3C. port1
- D. port4

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

FortiSandbox reserves port1 for device management and port3 for scanned files to access the Internet. Port1, port3 Reference:

https://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%20Input/500_Sniffer/100_Sniffer.htm

QUESTION 18 Which threats can FortiSandbox inspect when it is deployed in sniffer mode? (Choose three.)

- A. Spam emails
- B. Known malware
- C. Encrypted files
- D. Malicious URLs
- E. Botnet connections



Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19 Which FortiSandbox diagnostic command should you use to diagnose Internet connectivity issues on **port3**?

- A. ping
- B. tcpdump
- C. test-network
- D. traceroute

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://dokumen.tips/documents/fortios-54-cookbook-fortinet-docs-fortinetknowledgebase-technicaldocumentation-.html>

QUESTION 20 What information does a scan job report include? (Choose two.)

- A. Updates to the antivirus database
- B. Summary of the file activity
- C. Details about system files deleted or modified
- D. Changes to the FortiSandbox configuration

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Examine the CLI configuration, then answer the following question:

```
config system fortisandbox
set scan-order antispam-sandbox-content
end
```

Which of the following statements is true regarding this FortiMail's inspection behavior?

- A. Malicious URLs will be removed by antispam and replaced with a message.
- B. Suspicious files not detected by antivirus will be inspected by FortiSandbox.
- C. Known malicious URLs will be inspected by FortiSandbox.
- D. Files are skipped by content profile will be inspected by FortiSandbox.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22 What advantage does sandboxing provide over traditional virus detection methods?

- A. Heuristics detection that can detect new variants of existing viruses.
- B. Pattern-based detection that can catch multiple variants of a virus.
- C. Full code execution in an isolated and protected environment.
- D. Code emulation as packets are handled in real-time.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Heuristic analysis is capable of **detecting** many previously unknown **viruses** and **new variants** of current **viruses**. However, **heuristic** analysis operates on the basis of experience (by comparing the suspicious file **to** the code and functions of known **viruses**)

Reference: https://en.wikipedia.org/wiki/Heuristic_analysis

QUESTION 23 Which FortiWeb feature supports file submission to FortiSandbox?

- A. Attack signature
- B. Credential stuffing defense
- C. IP reputation
- D. File security

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24 Which of the following actions are performed by FortiSandbox at the static analysis stage?

- A. All activity is monitored and recorded while the sample is executed in a virtual environment.
- B. The sample's file type is determined and submitted into the appropriate scan job queue.
- C. The sample behavior is analyzed and embedded objects are extracted for analysis.
- D. Embedded attachments are scanned using the FortiGuard antivirus engine and the latest signature database.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Examine the FortiGate antivirus log detail shown in the exhibit, then answer the following question:

<div> <div></div> <div>AntiVirus</div> </div>	
Profile Name	AV-AcmeCorp
Virus/Botnet	FSA/RISK_HIGH
Virus ID	8
Reference	http://www.fortinet.com/ve?vn=FSA%2FRISK_HIGH
Detection Type	Virus
Direction	incoming
Quarantine Skip	File-was-not-quarantined.
FortiSandbox Checksum	90877c1f6e7c97fb11249dc28dd16a3a3ddfac935d4f38c
Submitted for FortiSandbox	false
Message	File reported infected by Sandbox.

Which of the following statements is true?

- A. FortiGate quarantined the file as a malware.
- B. The file matched a FortiSandbox-generated malware signature.
- C. The file was downloaded from www.fortinet.com.
- D. The **FSA/RISK_HIGH** verdict was generated by FortiSandbox.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Examine the virtual Simulator section of the scan job report shown in the exhibit, then answer the following question:

Action	CVE	Description	Method	Timestamp
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.313405
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.313733
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.313808
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.314096
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.314600
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.314657
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.314894
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.315164
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.315222
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.315397
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.315624
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.315679
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.315838
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.316091
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.316159

Based on the behavior observed by the virtual simulator, which of the following statements is the most likely scenario?

- A. The file contained a malicious image file.
- B. The file contained malicious JavaScript.
- C. The file contained a malicious macro.
- D. The file contained a malicious URL.

Correct Answer: B


Section: (none)

Explanation


Explanation/Reference:

QUESTION 27

Examine the scan job report shown in the exhibit, then answer the following question:

 **High Risk Trojan**

Mark as clean (false positive)


Received	Feb 14 2018 10:29:47
Started	Feb 14 2018 10:29:48-05:00
Status	Done
Rated By	VM Engine
Submit Type	Sniffer
Source IP	10.10.2.254
Destination IP	10.10.2.100
Digital Signature	No
Virus Total	


More Details


Suspicious Indicators


Behavior Summary


Analysis Details


 **WindowsXP**











 **WIN7X86VMO16E**

 **Captured Packets**

 **Original File**

 **Tracer Package**

 **Tracer Log**

-  **Behavior Chronology Chart**
-  **Suspicious Indicators (6)**
-  **Static Analysis (1)**
-  **Files Created (8)**
-  **Files Deleted (2)**
-  **Files Modified (1)**
-  **Launched Processes (2)**
-  **Registry Changes (3)**
-  **Network Behaviors (9)**
-  **Behaviors In Sequence (370)**

Tracker Package Version 02005.00514
Rating Package Version 02005.00507

Which of the following statements are true regarding this verdict? (Choose two.)

- A. The file contained malicious JavaScript.
- B. The file contained a malicious macro.
- C. The file was sandboxed in two-guest VMs.
- D. The file was extracted using sniffer-mode inspection.

Correct Answer: AC

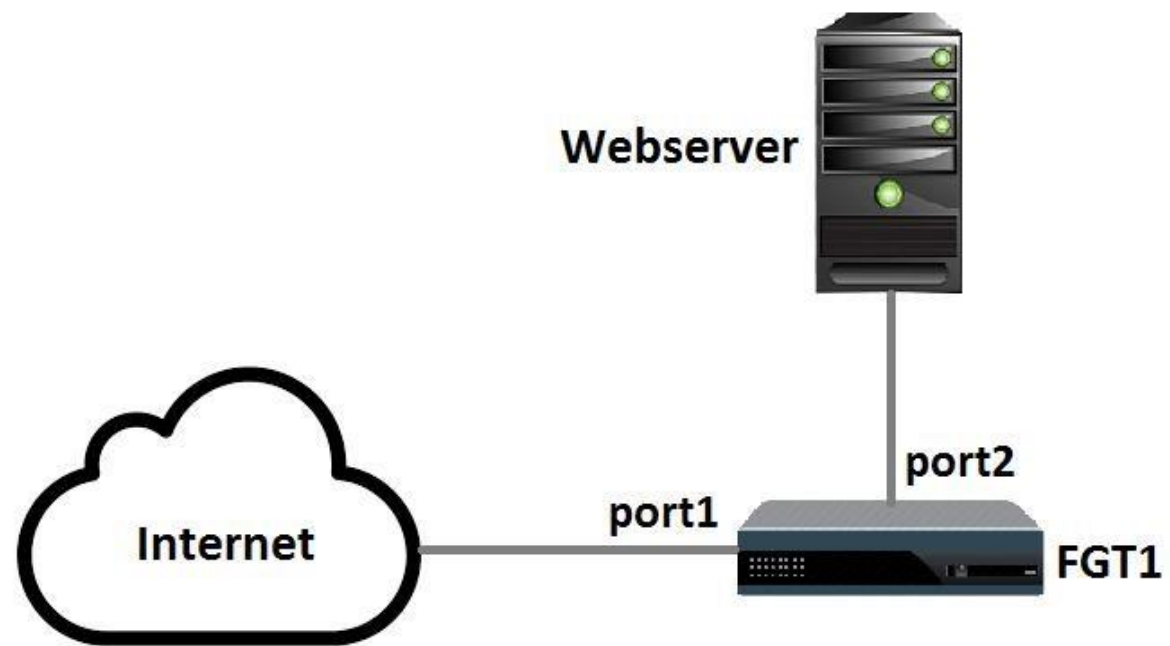
Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Examine the following topology shown in the exhibit, then answer the following question:



Which of the following configuration tasks are applicable to secure **Webservice** from known threats? (Choose two.)

- A. Apply an SSL inspection profile configured for protecting SSL server.
- B. Apply an antivirus profile to the **port1** -> **port2** firewall policy.
- C. Apply an SSL inspection profile configured for full SSL inspection.
- D. Apply a web filter profile to the **port1** -> **port2** firewall policy.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

Examine the FortiSandbox configuration on FortiMail shown in the exhibit, then answer the following question:

FortiSandbox

FortiSandbox Setting

FortiSandbox Inspection
☒ Statistics...

FortiSandbox type:

Appliance

Cloud

Server name/IP:

10.200.4.213

Test Connection

Notification email:

Statistics interval:

5

(minutes)

Scan timeout:

30

(minutes)

Scan result expires in:

60

(minutes)

What does the **Scan result expires in** value specify?

- A. How often the local scam results cache will expire on FortiMail.
- B. How long FortiMail will wait to send a file or URI to FortiSandbox.
- C. How long FortiMail will wait for a scan result from FortiSandbox.
- D. How long FortiMail will query FortiSandbox for a scan result.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30 Which of the following are FortiWeb's roles when integrated with FortiSandbox? (Choose two.)

- A. Share threat information
- B. Prevent outbreaks
- C. Generate a verdict
- D. Block known threats

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference: