



NSE7_ATP-2.5^{Q&As}

Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

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

https://www.geekcert.com/nse7_atp-2-5.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

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

QUESTION 2

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

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

QUESTION 3

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

QUESTION 4



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

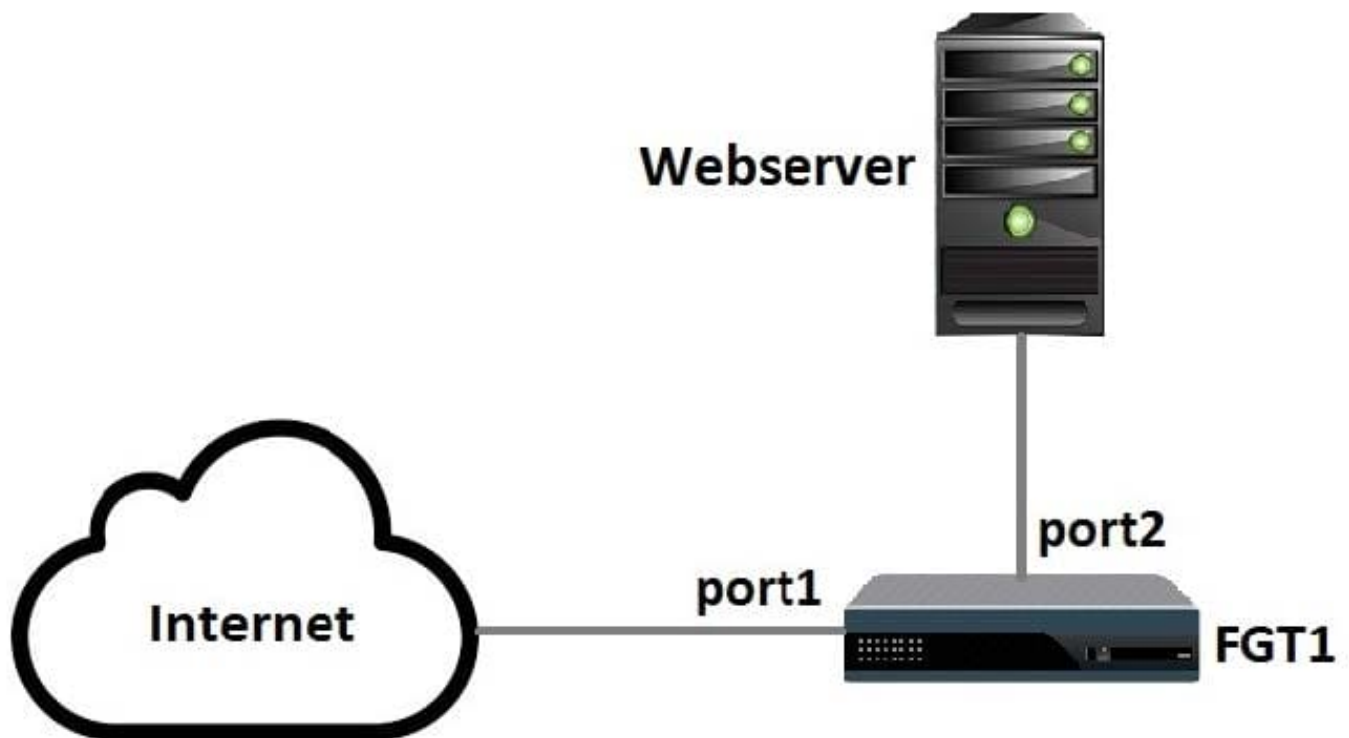
Based on the behavior observed by the virtual simulator, which of the following statements is the most likely scenario?

- 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

QUESTION 5

Examine the following topology shown in the exhibit, then answer the following question: Which of the following configuration tasks are applicable to secure Webserver 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

[NSE7_ATP-2.5 Practice Test](#)

[NSE7_ATP-2.5 Exam Questions](#)

[NSE7_ATP-2.5 Braindumps](#)