

# NSE7\_ATP-2.5<sup>Q&As</sup>

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.leads4pass.com/nse7\\_atp-2-5.html](https://www.leads4pass.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

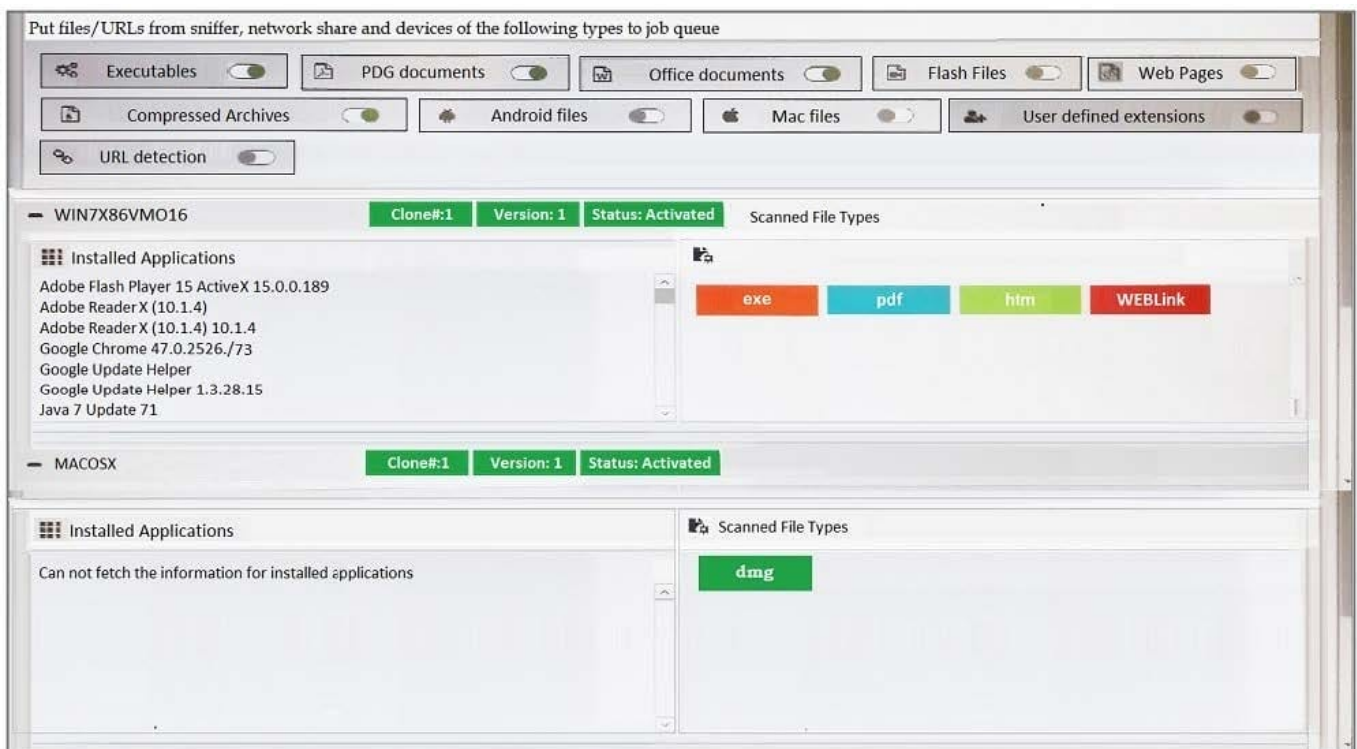
Which of the following are FortiWeb's roles when integrated with FortiSandbox? (Choose two.)

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

Correct Answer: AD

## QUESTION 2

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

**QUESTION 3**

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

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

AntiVirus	
Profile Name	AV-AcmeCorp
Virus/Botnet	FSA/RISK_HIGH
Virus ID	8
Reference	<a href="http://www.fortinet.com/ve?vn=FSA%2FRISK_HIGH">http://www.fortinet.com/ve?vn=FSA%2FRISK_HIGH</a>
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](http://www.fortinet.com).
- D. The FSA/RISK\_HIGH verdict was generated by FortiSandbox.

Correct Answer: C

[NSE7\\_ATP-2.5 PDF Dumps](#)

[NSE7\\_ATP-2.5 Practice Test](#)

[NSE7\\_ATP-2.5 Study Guide](#)