



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

### QUESTION 3

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

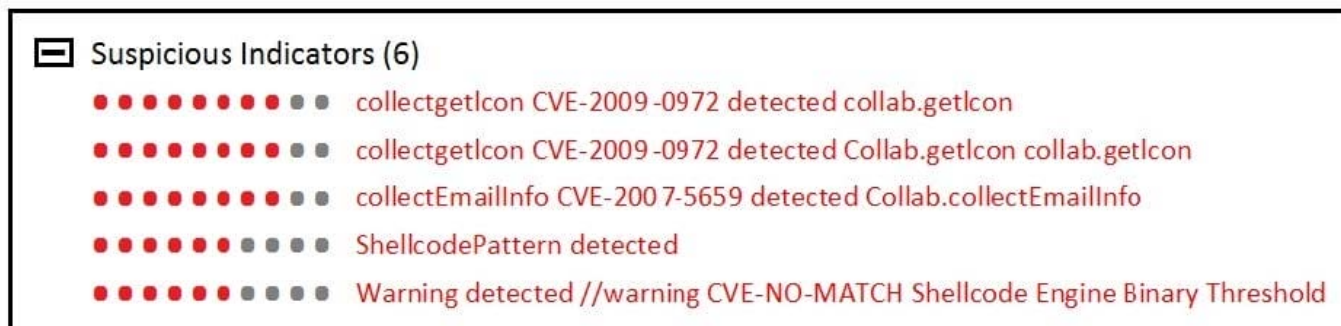
- A. Move clean files to a separate network share.
- B. Replace suspicious files with a replacement message.
- C. Detect malicious URLs.
- D. Detect network attacks.

Correct Answer: AB

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

### QUESTION 4

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

### 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	90877c1f6e7c97fb11249dc28dd16a3a3ddfacc935d4f38c
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

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

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

[NSE7\\_ATP-2.5 Exam Questions](#)