



# 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.geekcert.com/nse7\\_atp-2-5.html](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 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

### QUESTION 2

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

### QUESTION 3

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

**Enable FortiSandbox Detection & Analysis**

Address

Wait for FortiSandbox results before allowing file access  
Timeout:  seconds

Deny Access to file if sandbox is unreachable



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

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

---

#### QUESTION 4

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

---

#### 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

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

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