



# 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

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

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

---

### QUESTION 2

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 3

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

---

### QUESTION 4

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 5

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

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

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

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