



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.pass4itsure.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

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 2

Examine the scan job report shown in the exhibit, then answer the following question: Which of the following statements are true regarding this verdict? (Choose two.)

High Risk Trojan

Mark as clean (false positive)

Received: Feb 14 2018 10:29:47
Started: Feb 14 2018 10:29:48-05:00
Status: Done
Rated By: VM Engine
Submit Type: Sniffer
Source IP: 10.10.2.254
Destination IP: 10.10.2.100
Digital Signature: No
Virus Total: Q

More Details
Suspicious Indicators
Behavior Summary

Analysis Details

WindowsXP WINTX86/NO16E

Captured Packets Original File Tracer Package Tracer Log

Behavior Chronology Chart
Suspicious Indicators (6)
Static Analysis (1)
Files Created (8)
Files Deleted (2)
Files Modified (1)
Launched Processes (2)
Registry Changes (3)
Network Behaviors (9)
Behaviors In Sequence (370)

Tracker Package Version 02005.00514 Rating Package Version 02005.00507

- A. The file contained malicious JavaScript.
- B. The file contained a malicious macro.
- C. The file was sandboxed in two-guest VMs.
- D. The file was extracted using sniffer-mode inspection.

Correct Answer: AC

QUESTION 3



Which FortiWeb feature supports file submission to FortiSandbox?

- A. Attack signature
- B. Credential stuffing defense
- C. IP reputation
- D. File security

Correct Answer: C

QUESTION 4

Examine the FortiGate antivirus logs shown in the exhibit, then answer the following question:

#	Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
1	02-12 11:38	HTTP	10.0.1.10	fsa_dropper.exe	FSA/RISK_HIGH		host: 100.64.1.10	blocked
2	02-12 11:34	HTTP	10.0.1.10	fsa_downloader.exe	low risk		host: 100.64.1.10	monitored
3	02-12 11:30	HTTP	10.0.1.10	fsa_downloader.exe			host: 100.64.1.10	analytics
4	02-12 11:04	HTTP	10.0.1.10	fsa_sample_1.exe	clean		host: 100.64.1.10	monitored
5	02-12 11:00	HTTP	10.0.1.10	fsa_sample_1.exe			host: 100.64.1.10	analytics
6	02-12 11:00	HTTP	10.0.1.10	eicar.exe	EICAR_TEST_FILE		host: 100.64.1.10	blocked

Based on the logs shown, which of the following statements is correct? (Choose two.)

- A. The fsa_dropper.exe file was blocked using a local black list entry.
- B. The fsa_sample_1.exe file was not sent to FortiSandbox.
- C. The eicar.exe file was blocked using a FortiGuard generated signature.
- D. The fsa_downloader.exe file was not blocked by FortiGate.

Correct Answer: BD

File Filter allows the Web Filter profile to block files passing through a FortiGate based on file type. Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/610893/file-filter>

QUESTION 5

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/>

[Latest NSE7 ATP-2.5
Dumps](#)

[NSE7 ATP-2.5 Practice
Test](#)

[NSE7 ATP-2.5 Exam
Questions](#)