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.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

QUESTION 1

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 2

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

QUESTION 3

Which FortiSandbox interfaces can you use for sniffer mode? (Choose two.)

A. port2

B. port3

C. port1

D. port4

Correct Answer: BC

FortiSandbox reserves port1 for device management and port3 for scanned files to access the Internet.

Port1, port3

Reference: https://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%

20Input/500_Sniffer/100_Sniffer.htm

QUESTION 4

What advantage does sandboxing provide over traditional virus detection methods?

A. Heuristics detection that can detect new variants of existing viruses.

B. Pattern-based detection that can catch multiple variants of a virus.

C. Full code execution in an isolated and protected environment.

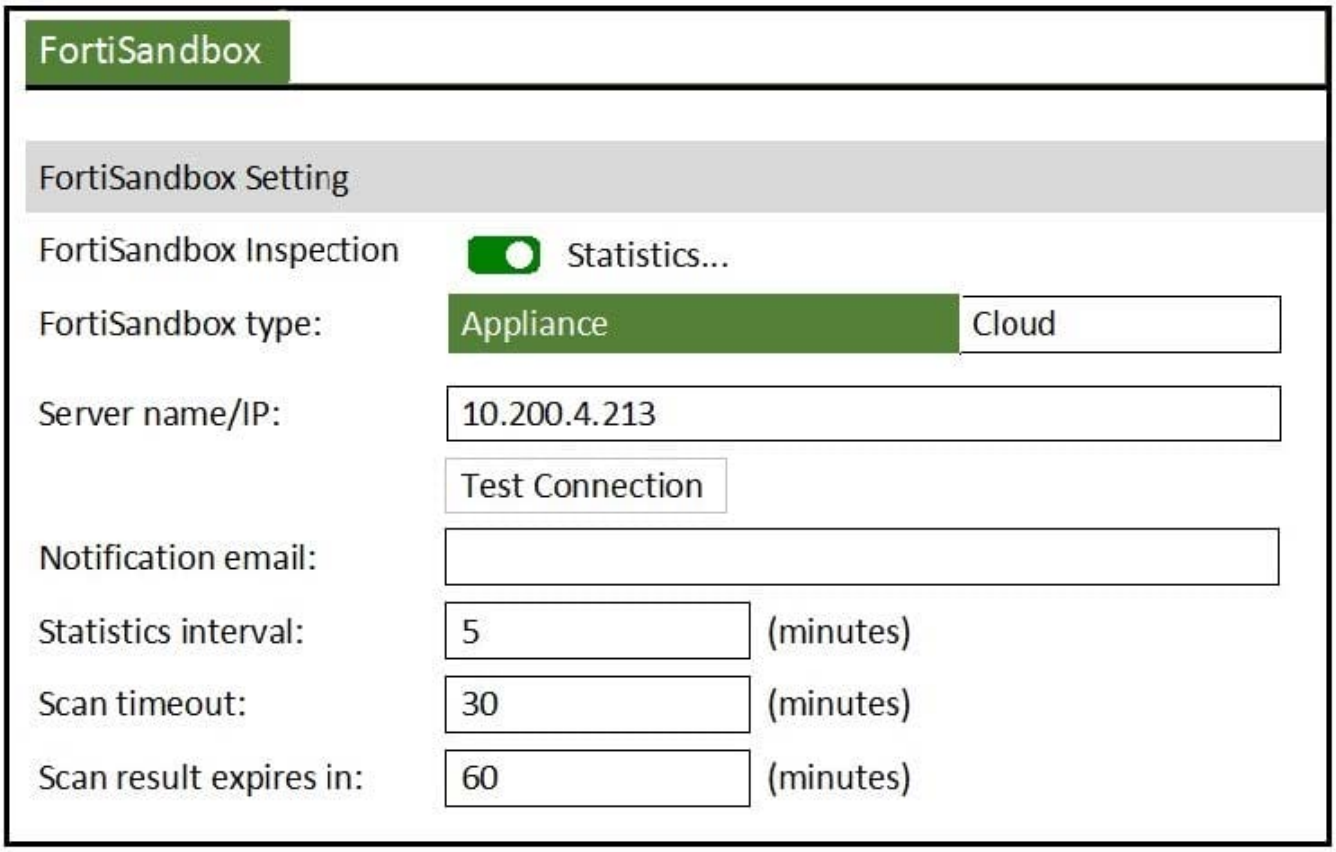
D. Code emulation as packets are handled in real-time.

Correct Answer: A

Heuristic analysis is capable of detecting many previously unknown viruses and new variants of current viruses. However, heuristic analysis operates on the basis of experience (by comparing the suspicious file to the code and functions of known viruses Reference: https://en.wikipedia.org/wiki/Heuristic_analysis

QUESTION 5

Examine the FortiSandbox configuration on FortiMail shown in the exhibit, then answer the following question:



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