NSE7_ATP-2.5$^{\text{Q\&As}}$

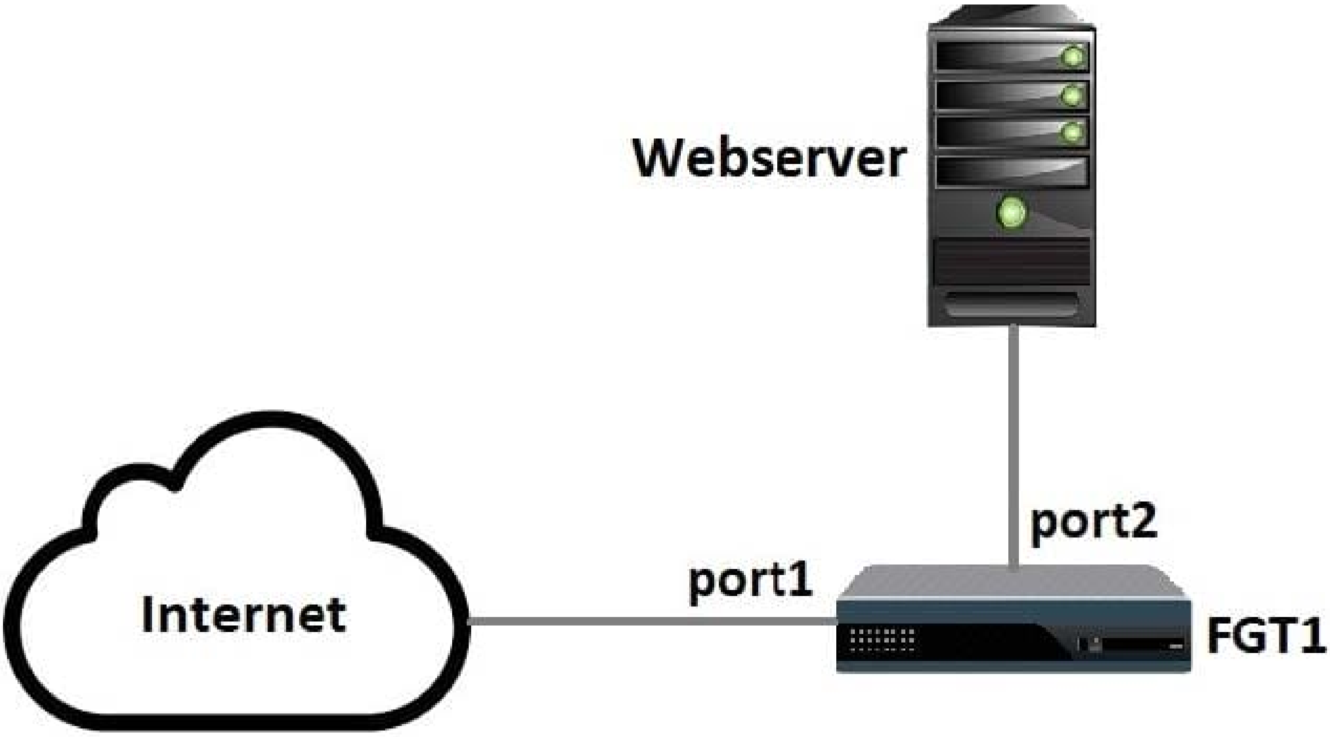
Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Examine the following topology shown in the exhibit, then answer the following question: Which of the following configuration tasks are applicable to secure Webserver from known threats? (Choose two.)



A. Apply an SSL inspection profile configured for protecting SSL server.

B. Apply an antivirus profile to the port1 -> port2 firewall policy.

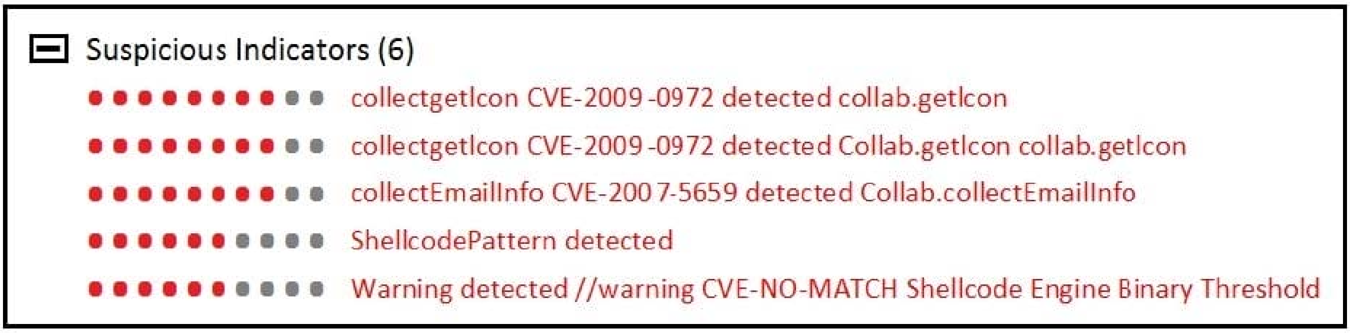
C. Apply an SSL inspection profile configured for full SSL inspection.

D. Apply a web filter profile to the port1 -> port2 firewall policy.

Correct Answer: AC

QUESTION 2

Examine the Suspicious Indicators section of the scan job shown in the exhibit, then answer the following question:



Suspicious Indicators (6)

●●●●●●●●○○ collectgetIcon CVE-2009-0972 detected collab.getIcon

●●●●●●●●○○ collectgetIcon CVE-2009-0972 detected Collab.getIcon collab.getIcon

●●●●●●●●○○ collectEmailInfo CVE-2007-5659 detected Collab.collectEmailInfo

●●●●●●○○○○ ShellcodePattern detected

●●●●●●○○○○ Warning detected //warning CVE-NO-MATCH Shellcode Engine Binary Threshold

Which FortiSandbox component identified the vulnerability exploits?

A. VM scan

B. Antivirus scan

C. Static analysis

D. Cache check

Correct Answer: C

QUESTION 3

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.

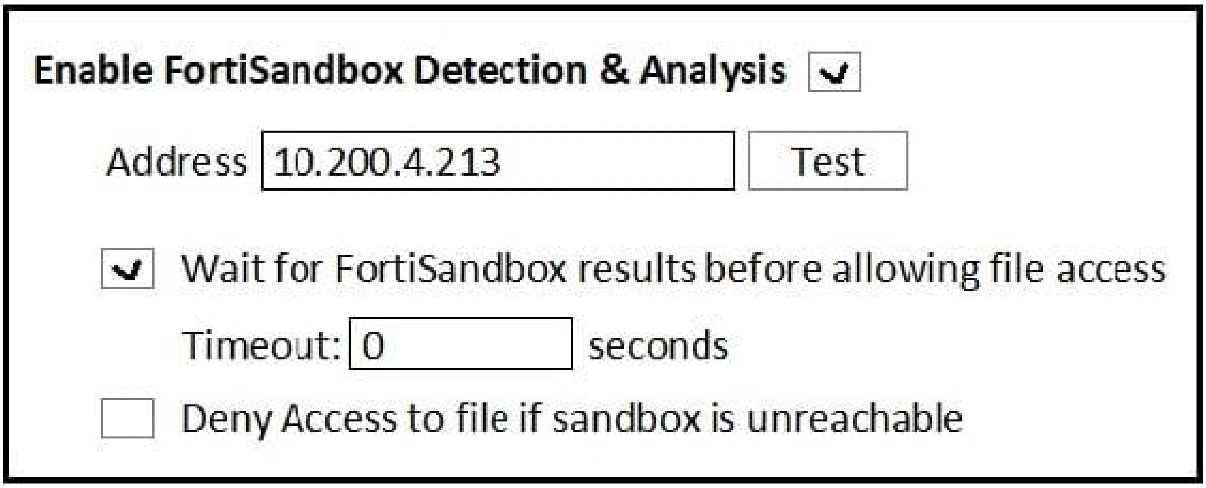
D. Code emulation as packets are handled in real-time.

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 4

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



Enable FortiSandbox Detection & Analysis ☑

Address 10.200.4.213 Test

☑ Wait for FortiSandbox results before allowing file access

Timeout: 0 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

QUESTION 5

Which of the kill chain stages does Fortinet\\'s advanced threat protection solution block? (Choose three.)

A. Command and control

B. Delivery

C. Reconnaissance

D. Lateral movement

E. Weaponization

Correct Answer: ACD