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

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.

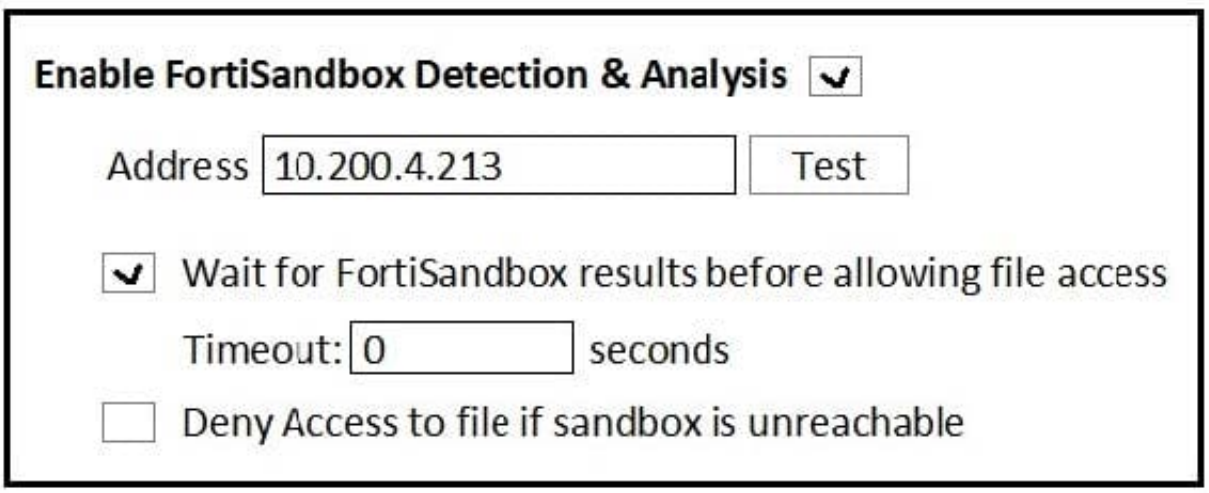
Port1, port3

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

20Input/500_Sniffer/100_Sniffer.htm

QUESTION 2

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



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 3

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

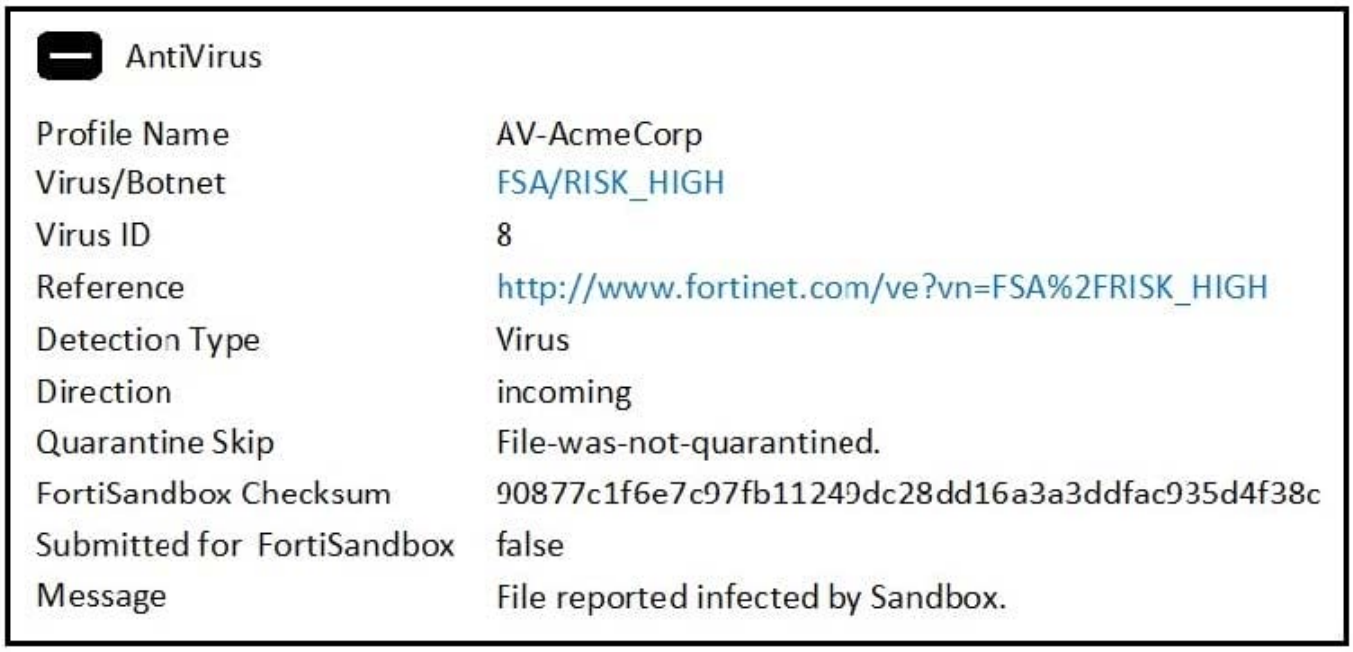
C. Lateral movement

D. Weaponization

Correct Answer: B

QUESTION 4

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



Which of the following statements is true?

A. FortiGate quarantined the file as a malware.

B. The file matched a FortiSandbox-generated malware signature.

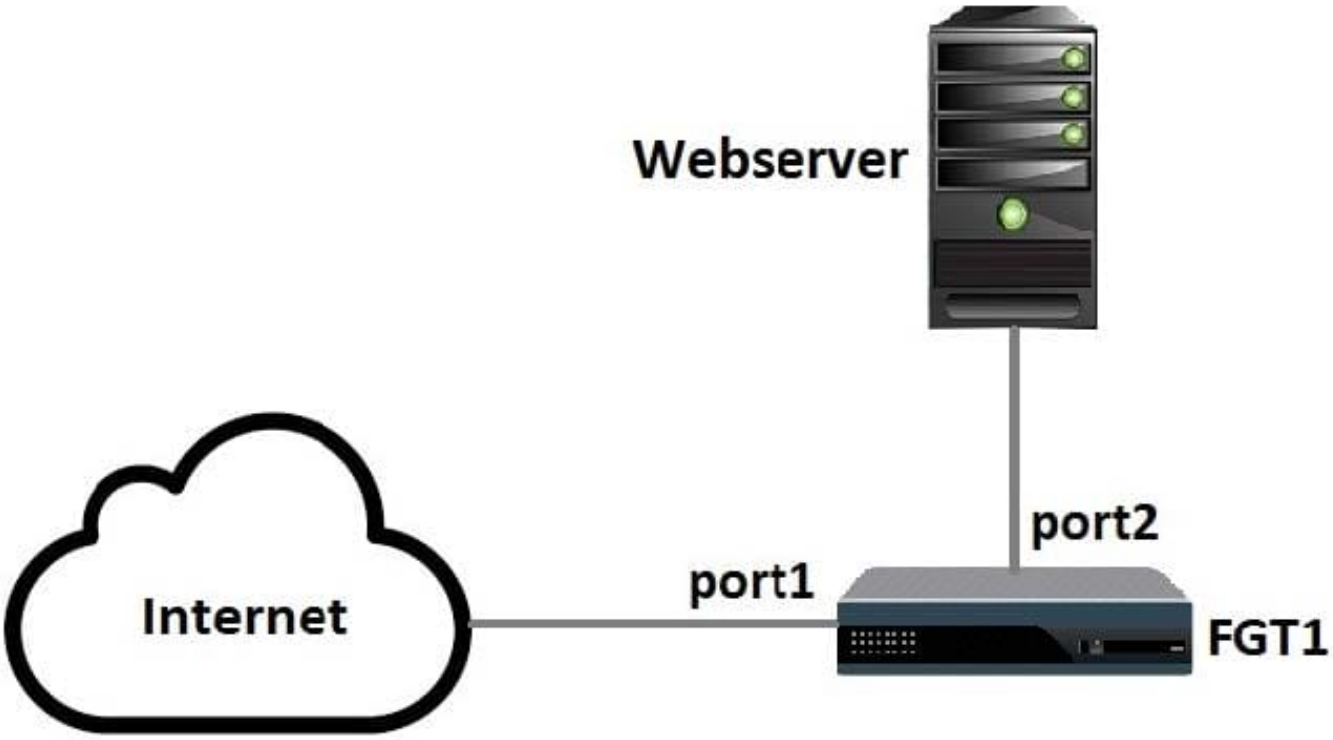
C. The file was downloaded from www.fortinet.com.

D. The FSA/RISK_HIGH verdict was generated by FortiSandbox.

Correct Answer: C

QUESTION 5

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