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.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

QUESTION 1

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 2

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.

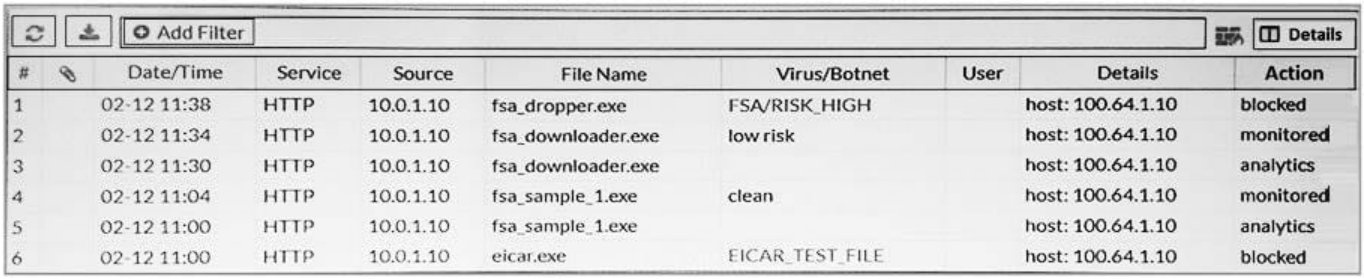
Port1, port3

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

20Input/500_Sniffer/100_Sniffer.htm

QUESTION 3

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



Add Filter | Details

#	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 FortiGiard 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 4

Which of the following advanced threat protection are capable of preventing patient-zero infections? (Choose two.)

A. FortiWeb and FortiSandbox

B. FortiClient and FortiSandbox

C. FortiMail and FortiSandbox

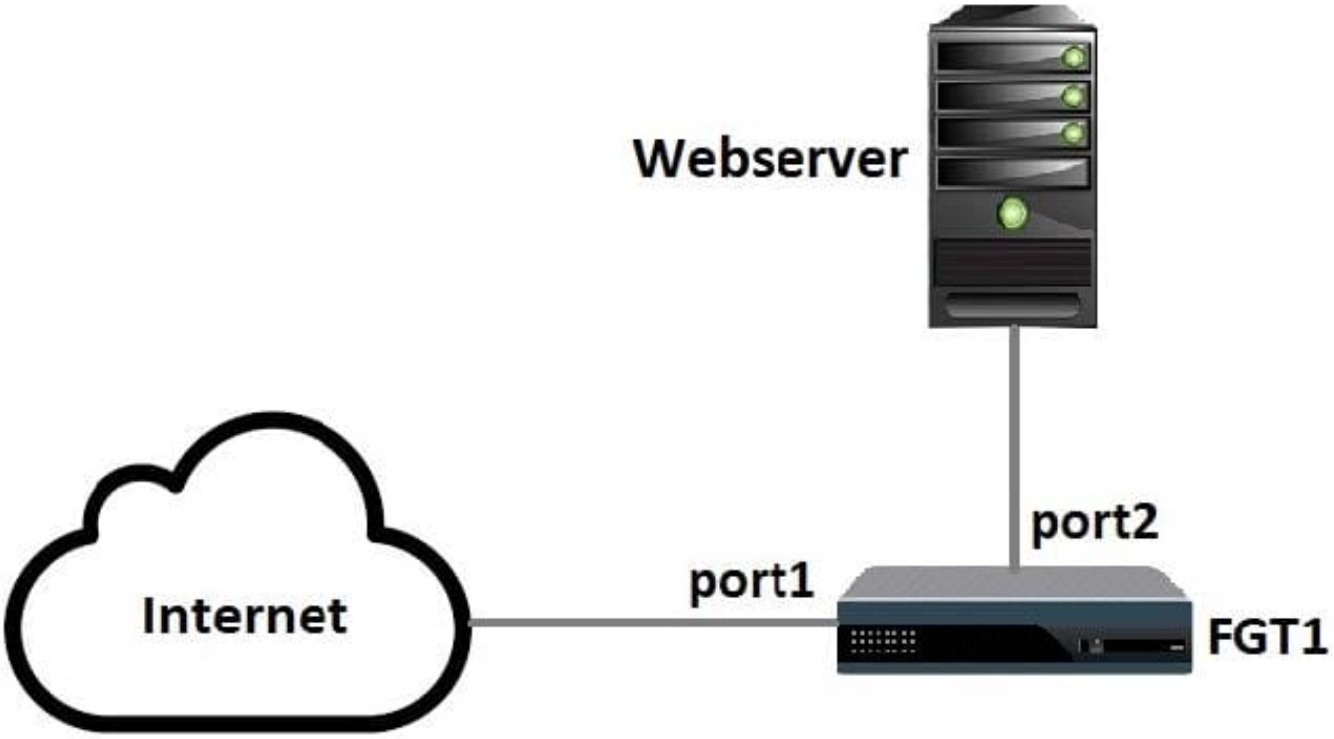
D. FortiGate and FortiSandbox

Correct Answer: AD

FortiGate Enterprise Firewall Platform provides the industry\\'s highest- performing firewall capabilities, and Fortinet\\'s FortiGuard Security Subscription Services provide the industry\\'s highest level of threat research, intelligence, and analytics. Reference: https://www.fortinet.com/content/dam/fortinet/assets/alliances/2019/sb-fortinet-allianceszifften.pdf

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