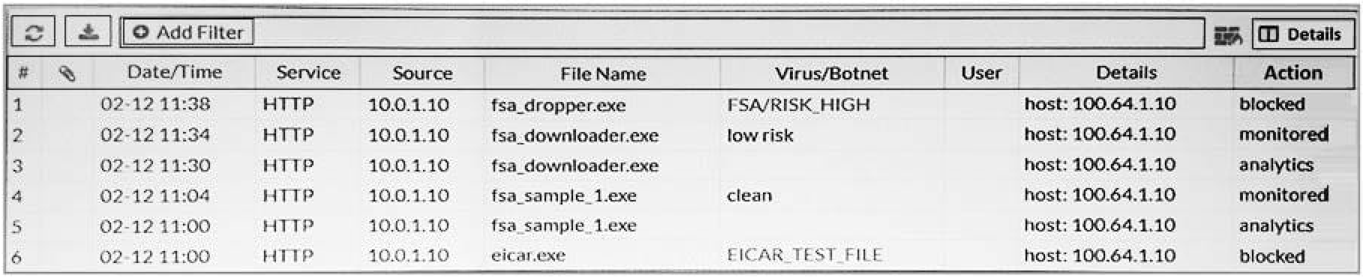
NSE7_ATP-2.5$^{\text{Q\&As}}$

Fortinet NSE 7 - Advanced Threat Protection 2.5

QUESTION 1

Examine the FortiGate antivirus logs shown in the exhibit, than 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 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 2

FortiSandbox generates structured threat information exchange (STIX) packages for which of the following threats? (Choose two.)

A. Botnet connections

B. Malware

C. Intrusion attempts

D. Malicious URLs

Correct Answer: AC

Reference: https://docs.fortinet.com/document/fortisandbox/3.0.3/administration-guide/170699/ioc-package

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

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 5

What information does a scan job report include? (Choose two.)

A. Updates to the antivirus database

B. Summary of the file activity

C. Details about system files deleted of modified

D. Changes to the FortiSandbox configuration

Correct Answer: BC