Fortinet FCP_FSA_AD-5.0 Mock Exam

Shared by Reilly on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A FortiGate root VDOM is authorized on FortiSandbox, and FortiGate is configured to send suspicious files to FortiSandbox for inspection. You create a new VDOM and then generates some traffic so that the new VDOM sends a file to FortiSandbox for the first time. In this scenario, which action will FortiSandbox take? (Choose one answer)

Options:

A- FortiSandbox will inspect all files, based on the root VDOM authorization state and configuration.
B- FortiSandbox will accept the file, but not inspect the file until the administrator manually authorizes the new VDOM on FortiSandbox.
C- FortiSandbox will authorize the new VDOM by default and inspect files as they are received.
D- FortiSandbox will accept the file; but not inspect the file until the administrator manually configures the new VDOM on FortiSandbox.

Answer:

B

Explanation:

The uploaded FortiSandbox 5.0 Administrator Study Guide states that each VDOM is handled independently by FortiSandbox, not under the root VDOM's authorization. It explicitly explains that ''each VDOM is treated as a separate input device on FortiSandbox'' and that each device must be authorized before FortiSandbox will process its submissions. It further adds that only when auto-authorization is enabled will FortiSandbox automatically authorize VDOMs as files are submitted.

Therefore, the new VDOM does not inherit the root VDOM's authorized state. Since the question does not say that auto-authorization is enabled, FortiSandbox will not automatically trust or process that new VDOM as if it were already approved. This eliminates A and C. Option D is incorrect because the issue is not that the administrator must manually configure the VDOM on FortiSandbox; the study guide specifically identifies authorization as the required control. For that reason, B is the best answer: the new VDOM must be manually authorized before its submitted files are inspected.

Question 2

Question Type: MultipleChoice

A FortiSandbox HA cluster is configured with the MTA adapter. What does the primary node do when it receives MTA jobs? (Select one answer)

Options:

A- It distributes the MTA jobs to secondary members.
B- It distributes the MTA jobs to itself or to worker nodes.
C- It assigns the MTA jobs to itself
D- It assigns the MTA jobs only to worker members.

Answer:

B

Explanation:

The Study Guide states that in an HA cluster, ''As well as normal scanning duties, the primary node also manages the cluster, distributes jobs, and gathers the verdicts.'' It also says that ''The worker nodes provide load balancing. The primary node distributes scan jobs to the worker nodes.''

From those official statements, the primary node is not just a coordinator. It also performs normal scanning duties itself, while distributing scan jobs across worker nodes for load balancing. That rules out A, because the secondary node is for failover, not normal job distribution. It rules out C, because the primary is not restricted to itself only. It also rules out D, because the primary can still perform scanning duties and is not limited to sending all jobs only to workers. Therefore, when the primary receives MTA jobs, the correct behavior is that it distributes the MTA jobs to itself or to worker nodes.

Question 3

Question Type: MultipleChoice

A FortiSandbox VM has been deployed and has been functioning correctly for several months. Suddenly, the system begins rejecting file submissions with an error message indicating a licensing problem. How can you determine, using the CLI, if the license is still valid? (Choose one answer)

Options:

A- vm-status
B- hc-setting -1
C- vm-license -1
D- status

Answer:

D

Explanation:

From the Deployment and System Settings lesson, the Study Guide explicitly states:

'The status command shows information about the system, including firmware level, device serial number, disk usage, Windows VM status, states of the boot and data disks, and more. For VM appliances, it will also show the FortiSandbox license status.'

The key phrase is 'For VM appliances, it will also show the FortiSandbox license status' --- making the status command the correct choice for verifying license validity on a FortiSandbox VM deployment.

While vm-license -l shows installed Windows/Microsoft Office license keys, and vm-status shows guest VM image information, neither directly reports on the FortiSandbox appliance license validity. The status command is the definitive command for checking overall system and license status.

Question 4

Question Type: MultipleChoice

Which stage of the Cyber Kill Chain does FortiSandbox and FortiClient EMS integration help to block? (Choose one answer)

Options:

A- Delivery
B- Weaponization
C- Reconnaissance

D- Command and control

Answer:

A

Explanation:

From the FortiClient EMS Integration lesson, the Study Guide states that FortiSandbox and FortiClient EMS integration helps break the kill chain by monitoring all downloads, removable media, mapped network drives, and email client file downloads --- intercepting threats at the Delivery stage before they can execute on the endpoint.

Additionally, from the Attack Methodologies section: 'When a USB is attached to a host protected with FortiClient, FortiClient can send the files on the USB drive to FortiSandbox for analysis, before allowing the user access to the files' --- further confirming the Delivery stage focus.

Question 5

Question Type: MultipleChoice

Which two products integrated with FortiSandbox work to protect against the lateral movement stage of the Cyber Kill Chain? (Select two answers)

Options:

A- FortiMail
B- FortiDeceptor
C- FortiADC
D- FortiGate

Answer:

B, D

Explanation:

From the Attack Methodologies lesson, the Study Guide explicitly states:

'During the lateral movement stage, the attacker is trying to compromise and infect other computers in the network. If these computers are protected with FortiClient, FortiClient can send

any file that the computer downloads, to FortiSandbox for analysis.'

'FortiDeceptor creates a network of decoys, to lure attackers and monitor their activities on the network. When attackers attack a decoy, an alert is generated. FortiDeceptor engages FortiSandBox to get a verdict on the suspected malware.'

'If you deploy FortiGate as an ISFW firewall, FortiGate can analyze the traffic moving across subnets and send any files to FortiSandbox for analysis to prevent propagation.'

Both FortiDeceptor (Option B) and FortiGate (Option D) are specifically identified as protecting against the lateral movement stage through their FortiSandbox integration.

Question 6

Question Type: MultipleChoice

What is the default timeout value on FortiGate for inline scanning mode? (Choose one answer)

Options:

A- 300 seconds
B- 50 seconds
C- 40 minutes
D- 30 minutes

Answer:

B

Explanation:

The correct answer is B. 50 seconds. The Study Guide explicitly states: ''FortiGate holds the file while waiting for a verdict from FortiSandbox... The default file inspection timeout, and maximum, is 50 seconds.'' This is the clearest direct statement for the default timeout used with inline scanning mode on FortiGate.

The Lab Guide confirms the same design limit from the operational side. During the inline scanning exercise, it notes: ''Because of the inline scanning time-out limit (maximum of 50 seconds), it's not recommended to submit files for VM inspection.'' That reinforces that inline scanning is designed for quick decision phases such as active content, community cloud, antivirus, and static analysis, not long VM dynamic analysis jobs. Therefore, options A, C, and D are incorrect because they are far above the documented inline inspection limit. The default

FortiGate inline scanning timeout is 50 seconds.

P2P exams