Fortinet

FCP_FSA_AD-5.0

Fortinet NSE 5 - FortiSandbox 5.0 Administrator

Questions & Answers (Demo)

Version: 4.0

Question: 1

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

A. Delivery

B. Weaponization

C. Reconnaissance

D. Command and control

Answer: A

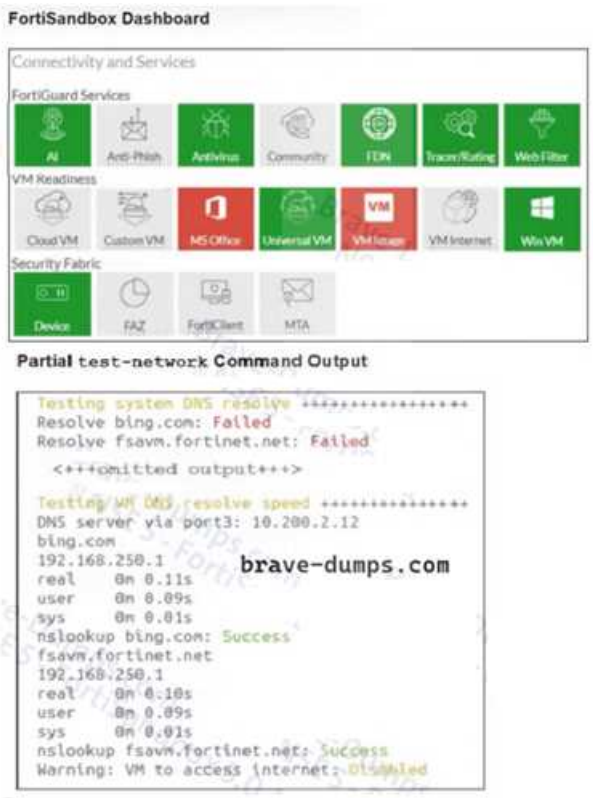
Explanation:

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: 2

Refer to the exhibits.



You are unable to download guest VMs on a new FortiSandbox VM. What is the reason for this? (Choose one answer)

A. FortiSandbox is using a private DNS server.

B. There is no internet connectivity on port1.

C. There is no internet connectivity on port3.

D. FortiSandbox does not have the necessary licenses.

Answer: B

Explanation:

From the Scanning and Rating Components lesson, the Study Guide explicitly states:

"VM images are downloaded from FortiGuard, using port1. So, you must ensure FortiSandbox has a default route and internet connectivity for port1."

The exhibit confirms this — the test-network output shows:

System DNS resolve: Failed for both bing.com and fsavm.fortinet.net

fsavm.fortinet.net is the FortiGuard VM image download server

This DNS failure on the system side (port1) confirms there is no internet connectivity on port1, preventing VM image downloads. Note that port3 internet shows "Warning: VM to access internet: Disabled" — but port3 is only for VM sandboxing traffic, not for downloading VM images.

Question: 3

You are asked to create some custom VMs to better represent your security environment. In which two FortiSandbox deployments is this supported? (Choose two answers)

A. Private cloud

B. Azure non-nested mode

C. Device-based

D. FortiSandbox Cloud

Answer: A, C

Explanation:

From the Scanning and Rating Components lesson, the Study Guide explicitly states:

"FortiSandbox allows you to modify the number of CPUs and memory assigned to a custom VM. This feature is supported on hardware models and private cloud VMs."

Hardware models = Device-based (Option C)

Private cloud VMs = Private cloud (Option A)

Azure non-nested mode and FortiSandbox Cloud do not support custom VM creation as per the Study Guide.

Question: 4

Which two statements are true about creating an API interface? (Choose two answers)

A. Ports configured for HA communication can also be configured as API ports.

B. API ports will not accept HTTP traffic.

C. The configuration must be performed using the CLI

D. The interface must also be designated as an administrative interface.

Answer: B, C

Explanation:

From the Lab Guide (Exercise 4 - Using Inline Scanning), the following is stated:

"FortiGate and FortiSandbox communicate through port 4443. Management or API ports grant access through port 4443."

And the CLI command used:

"Enter the following command to enable API access on port2: set api-port port2"

This confirms:

Option B is correct: Port 4443 uses HTTPS only — API ports will not accept HTTP traffic.

Option C is correct: The API port configuration must be performed using the CLI (set api-port port2), as there is no GUI option for this.

Option A is incorrect: The Study Guide states port3 cannot be a management port, and HA communication ports have dedicated roles that are not interchangeable with API ports.

Option D is incorrect: The CLI command sets the API port directly without requiring a separate administrative interface designation.

Question: 5

When using SIMNET, which two inspections cannot be performed with real traffic? (Choose two answers)

A. AV inspection

B. Dynamic scan

C. IP reputation

D. URL rating

Answer: A, C

Explanation:

From the Deployment and System Settings lesson, the Study Guide explicitly states what SIMNET cannot do with real traffic:

"When the malware attempts to download a file, FortiSandbox provides a fake download package. This allows the downloader to successfully execute; however, FortiSandbox cannot run its antivirus inspection on the file."

"If the malware creates a callback connection to an IP, FortiSandbox cannot rate the IP, to determine if it's a botnet server."

This confirms:

Option A (AV inspection) — Cannot be performed because SIMNET provides fake download packages, preventing real antivirus scanning

Option C (IP reputation) — Cannot be performed because SIMNET uses internal IPs for DNS responses, making IP reputation lookups meaningless against real botnet databases

Dynamic scan and URL rating can still occur inside the sandbox even without real internet access.