Fortinet.FCP_FSA_AD-5.0.v2026-07-01.q19

Exam Code:	FCP_FSA_AD-5.0
Exam Name:	FCP - FortiSandbox 5.0 Administrator
Certification Provider:	Fortinet
Free Question Number:	19
Version:	v2026-07-01
# of views:	104
# of Questions views:	190
https://www.freecram.net/torrent/Fortinet.FCP_FSA_AD-5.0.v2026-07-01.q19.html	

NEW QUESTION: 1
You are asked to configure FortiSandbox to use one VM instance for multiple sequential scan jobs without shutting down the instance between each scan job submission. Which scan profile setting must you enable to achieve this? (Choose one answer)
A. Adaptive VM scan
B. VM scan ratio
C. Parallel VM scan
D. Pipeline mode
Answer: (SHOW ANSWER)
From the Scanning and Rating Components lesson, the Study Guide explicitly states:
"The Pipeline Mode feature improves performance by allowing to scan multiple files, one at a time, without shutting down the VM instance after scanning each file."
"FortiSandbox will continue scanning files without shutting down the VM instance, as long as the VM status hasn't changed. If the VM status changes, then the VM instance will shut down and will be restored for the next job." This precisely matches the requirement - using one VM instance for multiple sequential scan jobs without shutting down between submissions. The other options serve different purposes:
Adaptive Scan dynamically adjusts clone numbers
VM Scan Ratio controls the percentage of jobs scanned in a VM
Parallel VM Scan runs multiple VMs simultaneously for a single job

NEW QUESTION: 2
You are asked to configure a FortiSandbox HA cluster. Port 4 on the primary and secondary nodes is dedicated for HA-specific communication. Which command must you use to configure the primary node? (Choose one answer)
A. hc-settings -sc -tN -nPrimaryNode -cFSAGrp -p -iport4
B. hc-settings -sc -tR -nPrimaryNode -cFSAGrp -p -iport4
C. hc-settings -sc -tF -nPrimaryNode -cFSAGrp -p -iport4
D. hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p -iport4
Answer: (SHOW ANSWER)

The Study Guide states that HA is configured from the CLI and that "the main HA cluster CLI commands are hc-settings, hc-slave, and hc-status". It also explains that "You use the hc-settings command and options to configure the main HA settings... node alias, group name, group password, and the HA interface." The same HA section further says that the primary and secondary nodes must have a dedicated HA communication interface, and specifically notes that "port4 in this example" is the HA interface between them.
On the primary-node example configuration shown on page 137 of the uploaded study guide, the command uses -tM for the primary node with -iport4 for the HA interface. That directly matches option D. The other options use different node-type flags and do not correspond to the primary-node example. Therefore, the correct command is hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p<password> -iport4.

NEW QUESTION: 3
You are troubleshooting long delays between FortiMail file submissions to FortiSandbox and verdicts being returned form FortiSandbox. Which FortiMail debug tool must you use to troubleshoot this issue further? (Choose one answer)
A. diagnose debug application hoststatd
B. diagnose debug application deferd
C. diagnose debug application oftpd
D. diagnose debug application mailfilterd
Answer: (SHOW ANSWER)
The FortiSandbox 5.0 Administrator Lab Guide shows that, when diagnosing FortiMail submission issues, the required FortiMail debugs are sandboxclid and deferd. It explicitly instructs: "Enter the following commands to enable both deferd and sandboxclid debugging" and then shows that the deferd daemon spools the email and later releases the email from the queue folder after FortiSandbox processing. Because sandboxclid is not one of the answer choices, the best answer among the listed FortiMail debug tools is deferd. It is the FortiMail daemon directly shown in the official lab workflow for troubleshooting submission-and-verdict handling. The other options in the answer list are not the ones the lab uses for FortiMail-to-FortiSandbox submission troubleshooting. So, based on the uploaded guide, diagnose debug application deferd is the correct choice.

NEW QUESTION: 4
A security analyst is reviewing a scan job report that indicates a true positive match. The job report displays that the malware attempts to replace vital system executables. Which type of malware is the analyst observing? (Choose one answer)
A. Exploit
B. Trojan
C. Dropper
D. Rootkit
Answer: (SHOW ANSWER)
The Results Analysis section gives direct malware-type definitions. It says: "A downloader attempts to download malicious content from a remote system", "A dropper installs malicious content", "A trojan appears to be a legitimate software application", and most importantly, "A rootkit attempts to hide its components by replacing valid system files." That exact wording matches the question statement about malware attempting to replace vital system executables. Replacing valid system files is classic rootkit behavior because the purpose is concealment and persistence by hiding malicious components behind trusted operating-system files. A dropper's main role is delivering payloads. A trojan is mainly deceptive software that appears legitimate. An exploit takes advantage of a vulnerability. None of those definitions match the described behavior as precisely as the rootkit definition in the Study Guide. Therefore, the malware type being observed is Rootkit.

NEW QUESTION: 5
There is a connectivity problem between FortiSandbox and the FortiGuard distribution servers. You observe that a firewall located between FortiSandbox and the internet allows traffic on ports TCP/4443, UDP/8888, and UDP/53. What is the cause of the issue? (Choose one answer)
A. They must allow TCP 443 out
B. They must allow TCP 8890 out
C. They must allow UDP 514 out
D. They must allow UDP 443 out
Answer: (SHOW ANSWER)
From the Deployment and System Settings lesson, the Study Guide states:
"The test-network command checks FortiGuard services as its last set of validation tests. These include the FortiGuard distribution network (FDN) accessibility, FDN contract expiration, web filtering service, and the community cloud service. All these FortiGuard services should be reachable and valid for FortiSandbox to be effective."
"The diagnose-debug fdn command provides details around FortiSandbox and the FortiGuard Distribution Network (FDN) communication and updates." FortiGuard Distribution Network (FDN) communication requires TCP/443 for HTTPS-based update and licensing communication. The current firewall rules allow TCP/4443 (API/management), UDP/8888 (FortiGuard queries), and UDP/53 (DNS), but TCP/443 is missing - which is the standard port required for FortiGuard FDN connectivity and license validation.

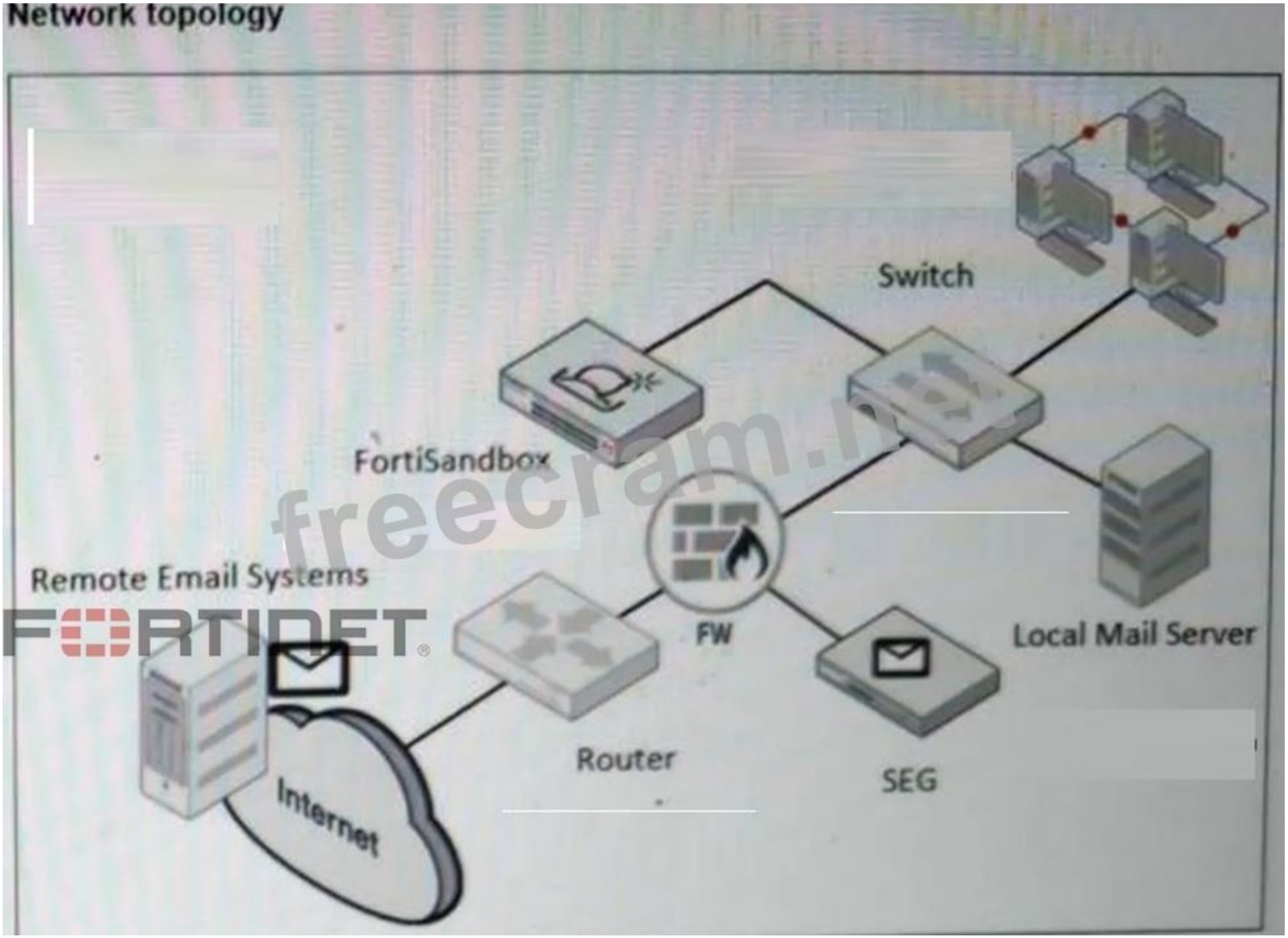
NEW QUESTION: 6
An organization has an existing FortiGate provisioned as a data center firewall (DCFW) that submits inbound files to FortiSandbox for inline scanning. As a result of a network redesign, traffic between the FortiSandbox and the DCFW now passes through an intermediate firewall. Inline scanning is no longer working. While examining the configuration of the intermediate firewall you notice that it is configured to allow traffic on ports TCP/3389, UDP/53, and TCP/443. What must you change for the integration to work? (Choose one answer)
A. FortiGate must be able to access FortiSandbox on TCP/4443.
B. FortiGate must be able to access FortiSandbox on TCP/8890.
C. FortiGate must be able to access FortiSandbox on UDP/8888.
D. FortiGate must be able to access FortiSandbox on UDP/1344.
Answer: (SHOW ANSWER)
The FortiSandbox 5.0 Administrator Lab Guide explicitly states during the inline scanning configuration: "FortiGate and FortiSandbox communicate through port 4443. Management or API ports grant access through port 4443." In the same exercise, the guide has you enable API access on port2 specifically so inline scanning can function, which confirms that the integration depends on FortiGate reaching FortiSandbox over TCP/4443.
In this scenario, the intermediate firewall currently allows TCP/3389, UDP/53, and TCP/443, but not TCP/4443. That is why inline scanning stopped working after the redesign. TCP/443 is not sufficient here because the documented FortiGate-to-FortiSandbox inline communication port is 4443, not standard HTTPS 443. The other ports in the options do not match the inline-scanning communication requirement described in the uploaded lab materials. Therefore, the required fix is to allow FortiGate access to FortiSandbox on TCP/4443.

NEW QUESTION: 7
Which two products integrated with FortiSandbox work to protect against the lateral movement stage of the Cyber Kill Chain? (Choose two answers)

A. FortiMail
B. FortiDeceptor
C. FortiADC
D. FortiGate
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 8
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: (SHOW ANSWER)
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.

NEW QUESTION: 9
Refer to the exhibit.



A network topology is shown. Which two important steps must you take before you enable a BCC adapter on FortiSandbox? (Choose two answers)

A. Configure the upstream SEG to extract files and URLs from emails and send them to FortiSandbox for analysis.

B. Configure an A record on the DNS server for the FortiSandbox IP.

C. Configure the sub-domain on the upstream SEG to BCC emails to FortiSandbox.

D. Add an MX record on the DNS server for the BCC email sub-domain to resolve to the FortiSandbox IP.

Answer: (SHOW ANSWER)

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

"You can submit emails from an upstream MTA server to FortiSandbox using a BCC adapter. FortiSandbox will extract attachment files and URLs in an email body." For a BCC adapter to function correctly, two critical prerequisites must be in place:

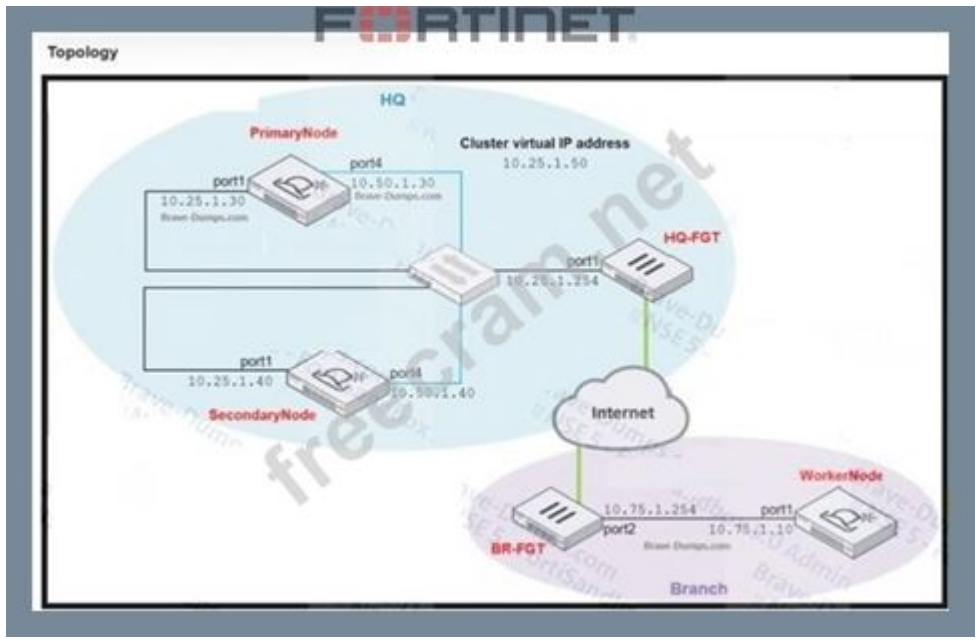
Option C - The upstream SEG must be configured to BCC emails to a FortiSandbox sub-domain so that email copies are routed to FortiSandbox for analysis Option D - An MX record must be added to the DNS server for the BCC email sub-domain, so that the sub-domain resolves to the FortiSandbox IP address, allowing the SEG to properly deliver BCC email copies Option A is incorrect because the BCC adapter handles full email inspection - FortiSandbox itself extracts files and URLs rather than the SEG doing this. Option B is incorrect because an MX record (not just an A record) is the required DNS configuration for email routing.

NEW QUESTION: 10

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: (SHOW ANSWER)
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.

NEW QUESTION: 11
Refer to the exhibit.



Which command must you use to configure the worker node? (Choose one answer)
A. hc-worker -a -sI0.50.1.30 -p<password>
B. hc-worker -a -sI0.25.1.50 -p<password>
C. hc-worker -a -sI0.75.1.254 -p<password>
D. hc-worker -a -sI0.25.1.30 -p<password>

Answer: (SHOW ANSWER)
From the High Availability and Management lesson, the Study Guide states:
"You must configure the HA group name, password, and the cluster virtual IP. The worker nodes provide load balancing. The primary node distributes scan jobs to the worker nodes."
"You must configure the HA group name, password, and the virtual IP only on the primary node... Devices will interact with the cluster using this virtual IP." From the exhibit topology:
Cluster Virtual IP address = 10.25.1.50
Primary Node port1 = 10.25.1.30
Secondary Node port1 = 10.25.1.40
Worker Node port1 = 10.75.1.10
The worker node must be configured to point to the Cluster Virtual IP (10.25.1.50), not the individual primary node IP. This is because worker nodes join the cluster by connecting to the cluster virtual IP address.
Therefore the correct command is: hc-worker -a -sI0.25.1.50 -p<password>

NEW QUESTION: 12
To assign a file to a VM image, which two conditions must be true? (Choose two answers)
A. FortiSandbox must have the appropriate license entitlements.
B. The VM image clone value must be a non-zero number.
C. The file type must be configured to enter the job queue.
D. The VM image must have the software required to open the file.
Answer: (SHOW ANSWER)
From the Scanning and Rating Components lesson, the Study Guide explicitly states:
"The second section of the Scan Profile, VM Association, allows you to define file extensions and VM image associations. This means that specific files are sandboxed by the associated VM image. To assign a file to a VM image, the following conditions must be true:
The file type must be configured to enter the job queue (first section of the scan profile).
The VM image clone value cannot be a non-zero number."
This directly confirms:
Option B - The VM image clone value must be a non-zero number (clones must be allocated) Option C - The file type must be configured to enter the job queue via the scan profile Pre-Filter section Options A and D, while potentially relevant in practice, are not listed as the two required conditions in the Study Guide.

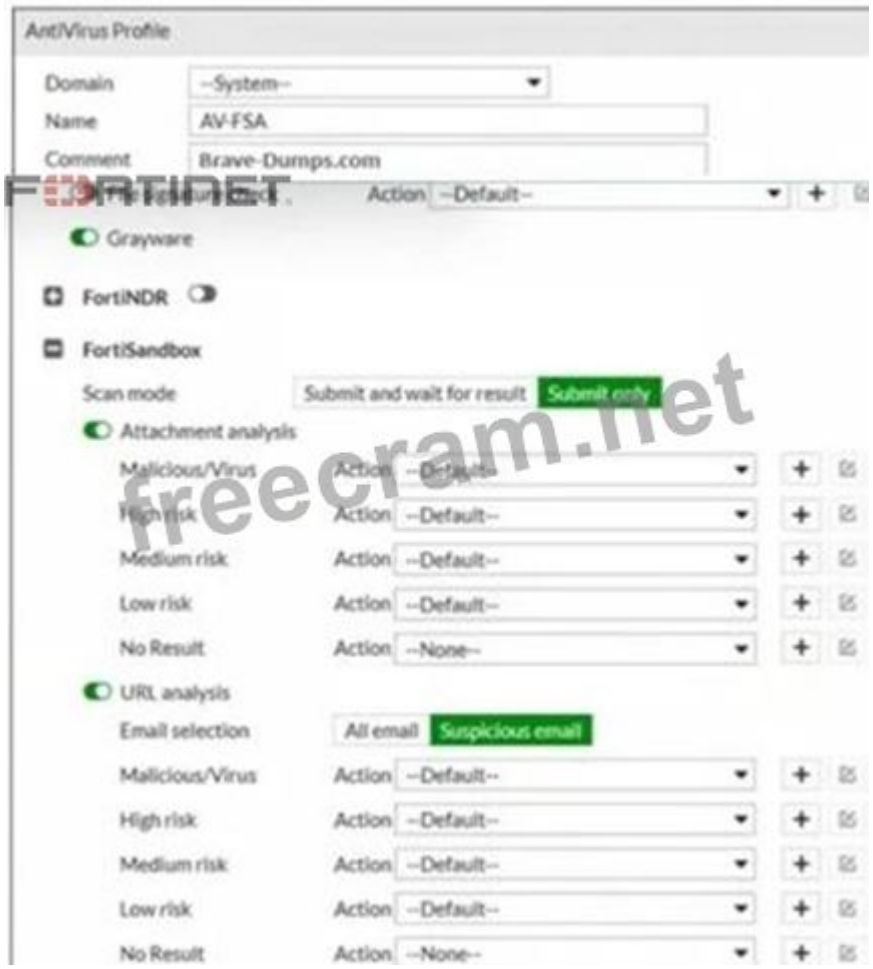
NEW QUESTION: 13
Refer to the exhibit.


Which two inspections will FortiSandbox perform on samples submitted for sandboxing? (Choose two answers)

A. IP reputation check on callback connections
B. Antivirus inspection on downloaded files
C. URL rating on HTTP GET requests
D. URL rating on FQDN seen in DNS requests
Answer: (SHOW ANSWER)
The exhibit shows the Connectivity and Services widget with VM Internet = GRAY (disabled) while Web Filter = GREEN (enabled) and Tracer/Rating = GREEN (enabled).
Since VM Internet access is disabled (SIMNET mode), the Study Guide explicitly states what CANNOT be performed:
"When the malware does a DNS query, FortiSandbox responds with an internal IP address. Performing an IP reputation lookup on an internal IP would be meaningless." - eliminates Option A
"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." - eliminates Option B
"If the malware creates a callback connection to an IP, FortiSandbox cannot rate the IP, to determine if it's a botnet server." However, the Study Guide confirms URL rating CAN still be performed:
"FortiSandbox checks connection attempts to any URLs against the FortiGuard web filtering database."
"Similarly, FortiSandbox assesses all IP connection attempts against the FortiGuard IP rating database to identify known command-and-control (C&C) servers." Since the Web Filter service is GREEN (active), FortiSandbox can still:
Option C - Perform URL rating on HTTP GET requests using the FortiGuard web filtering database Option D - Perform URL rating on FQDN seen in DNS requests using the FortiGuard web filtering database These URL rating inspections use FortiSandbox's own internet connectivity (port1) to query FortiGuard, independent of the VM internet access status on port3.

NEW QUESTION: 14
Review the exhibits.

FortiMail Antivirus Profile Configuration



A FortiMail device is integrated with a FortiSandbox device. What is the expected behavior on FortiMail for emails that require FortiSandbox inspection? (Choose one answer)

A. FortiMail will queue emails for up to 5 minutes during URL rating errors before submitting URLs to FortiSandbox

B. FortiMail will queue emails for up to 30 minutes to allow FortiSandbox to finish scanning all attachments and URLs.

C. FortiMail will not send attachments and URLs to FortiSandbox if their rating exists in the local cache.

D. FortiMail will deliver all emails to the destination after the emails pass all local security checks.

Answer: (SHOW ANSWER)

From the FortiMail Integration lesson, the Study Guide explicitly states:

"The Scan timeout value determines how long FortiMail will wait for a response from FortiSandbox. The default is 30 minutes. So, if after 30 minutes FortiSandbox is unable to generate a verdict, FortiMail will release the email to the end user."

"SMTP is a store-and-forward protocol. This allows FortiMail to queue the email while FortiSandbox inspects all submitted samples. FortiMail will release the email only if there is a scan timeout event, or FortiSandbox returns a clean verdict." The Integration Settings exhibit clearly confirms Scan timeout = 30 minutes, and the AV Profile shows both Attachment analysis and URL analysis are enabled - meaning FortiMail will hold/queue emails for up to 30 minutes while FortiSandbox completes inspection of all attachments and URLs before taking action.

NEW QUESTION: 15

You notice a recent file downloaded by some end stations is exhibiting malware behavior, however, on the sandbox the file is rated clean. After further investigation you determine that only end stations using the Opera browser are being affected. What must you do to prevent these infections? (Choose one answer)

A. Enable the STIX/TAXII Integration setting on FortiSandbox.
B. Configure a custom VM to use the same browser as the exploited end stations.
C. Modify the scan profile to include the malware file type.
D. Change the job queue priority to process web-based files first.
Answer: (SHOW ANSWER)
The best answer is B. The Study Guide explains that under VM settings, "FortiSandbox has a Browser selection that allows you to choose which internet browser the VM instance will use. This helps to customize the test using an internet browser that more closely resembles the user's environment or just monitor if the test delivers different results." It also states that the default browser choices are Internet Explorer, Firefox, Chrome, and Edge. In addition, the guide says that "The VM images provided by Fortinet might not suit your needs... You can generate a custom VM that fits your organization's needs and upload it to FortiSandbox." Because only endpoints using Opera are affected, the clean verdict likely occurred because the sandbox environment does not accurately reproduce the exploited browser environment. The most effective fix is to make the sandbox environment match the real target environment more closely by using a custom VM with the same browser behavior as the affected endpoints. The other answers do not address the root cause. STIX/TAXII is unrelated, changing the scan profile file type does not solve a browser-specific exploit path, and job queue priority affects order, not analysis fidelity. Therefore, the required action is to configure a custom VM to use the same browser as the exploited end stations.

NEW QUESTION: 16
What is the default timeout value on FortiGate for inline scanning mode? (Choose one answer)
A. 300 seconds
B. 50 seconds
C. 40 minutes
D. 30 minutes
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 17

You are configuring an integration between FortiWeb and FortiSandbox. On FortiWeb, where must you define the settings to submit files to FortiSandbox? (Choose one answer)

A. File security

B. Attack signature

C. Web anti-defacement

D. Antivirus

Answer: (SHOW ANSWER)

From the FortiWeb Integration lesson, the Study Guide explicitly states:

"You can configure FortiSandbox file submission in a file security policy. Any files not detected by the FortiGuard antivirus engine will be uploaded to FortiSandbox."

"You can configure FortiWeb to send attachments to FortiSandbox for additional scans to detect advanced persistent threats or zero-day attacks." From the Lab Guide (Exercise 1 - FortiWeb Integration):

"Click Web Protection > Input Validation > File Security. In the File Security Policy section, click Create New. Configure Send Files to FortiSandbox: Enabled." This confirms that File Security (Option A) is the correct location on FortiWeb to configure FortiSandbox file submission settings.

NEW QUESTION: 18

How can you limit an administrator's access to scan jobs on FortiSandbox based on the system that submitted the scan request? (Choose one answer)

A. By configuring device groups to assign to users

B. By configuring access in the log server configuration settings

C. By configuring netshare groups to define access

D. By configuring administrator profiles that define job access

Answer: D (LEAVE A REPLY)

The correct answer is D. The Study Guide states that FortiSandbox has default administrative profiles and specifically says: "The Read Only profile is intended to be used for system-wide monitoring and reporting tasks, whereas the Device profile is intended to be used for monitoring alerts and reporting for a specific device." That wording directly matches the question requirement to limit access based on the system that submitted the scan request. In other words, FortiSandbox uses administrator profiles to control whether an admin can view broad system-wide activity or only jobs and alerts related to a specific submitting device.

This eliminates the other options. The Study Guide does not describe device groups, log server settings, or netshare groups as the mechanism for restricting admin visibility of scan jobs by submitter. Instead, access control is tied to the admin profile model. The Device profile is the exact fit because it narrows monitoring and reporting to a particular device context rather than the entire system. Therefore, the way to limit an administrator's access to scan jobs by the submitting system is by configuring administrator profiles that define job access.

NEW QUESTION: 19

To allow access to the FortiSandbox GUI the administrator must configure an IP address and a default gateway. Which two commands must the administrator use to accomplish this task? (Choose two answers)

A. set default-gw <IP Address>

B. set api-port port1

C. set admin-port port1

D. set port1-ip <IP address>

Answer: (SHOW ANSWER)

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

"Initial port1 IP configuration must be performed from the console, using the commands shown on this slide. If your management computer is on a separate subnet from FortiSandbox, you must specify a gateway address using the commands shown on this slide."

The two required commands are:

set port1-ip <IP address> - to assign the IP address to port1 for GUI access set default-gw <IP Address> - to configure the default gateway so the management computer can reach FortiSandbox from a different subnet Option B (set api-port port1) is for API access configuration, and Option C (set admin-port port1) is not a valid FortiSandbox CLI command for this purpose.