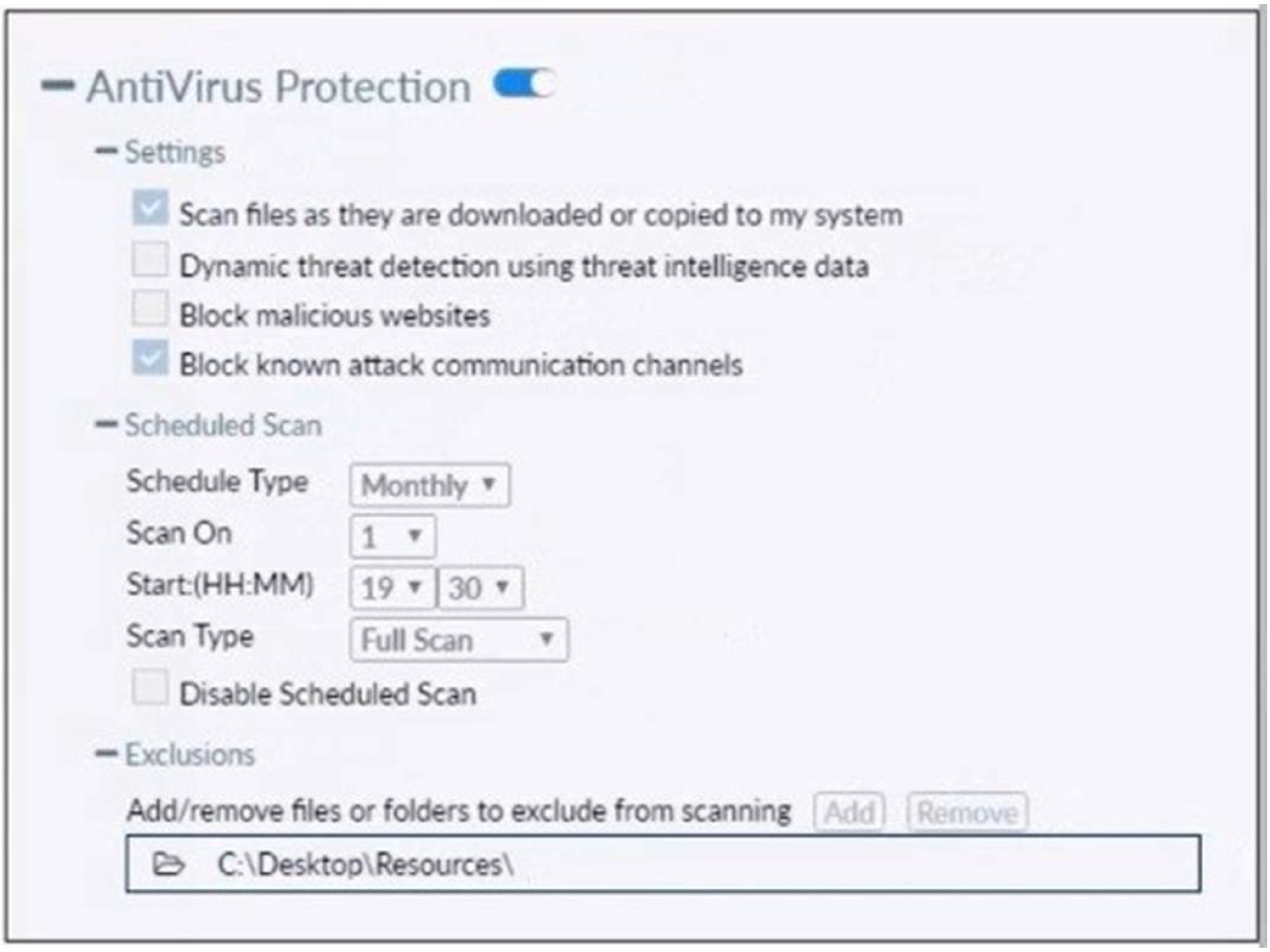
Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

NEW QUESTION 1
Refer to the exhibit.



AntiVirus Protection

Settings

☑ Scan files as they are downloaded or copied to my system
□ Dynamic threat detection using threat intelligence data
□ Block malicious websites
☑ Block known attack communication channels

Scheduled Scan

Schedule Type: Monthly
Scan On: 1
Start:(HH:MM): 19 : 30
Scan Type: Full Scan
□ Disable Scheduled Scan

Exclusions

Add/remove files or folders to exclude from scanning

C:\Desktop\Resources\

Based on the settings shown in the exhibit which statement about FortiClient behavior is true?

A. FortiClient quarantines infected files and reviews later, after scanning them.
B. FortiClient blocks and deletes infected files after scanning them.
C. FortiClient scans infected files when the user copies files to the Resources folder
D. FortiClient copies infected files to the Resources folder without scanning them.

Answer: A

Explanation:
Action On Virus Discovery Warn the User If a Process Attempts to Access Infected Files Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. Deny Access to Infected Files Ignore Infected Files

NEW QUESTION 2
Which two statements are true about the ZTNA rule? (Choose two.)

A. It applies security profiles to protect traffic
B. It applies SNAT to protect traffic.
C. It defines the access proxy.
D. It enforces access control.

Answer: AD

Explanation:
? Understanding ZTNA Rule Configuration:
? Evaluating Rule Components:
? Eliminating Incorrect Options:
? Conclusion:
References:
? ZTNA rule configuration documentation from the study guides.

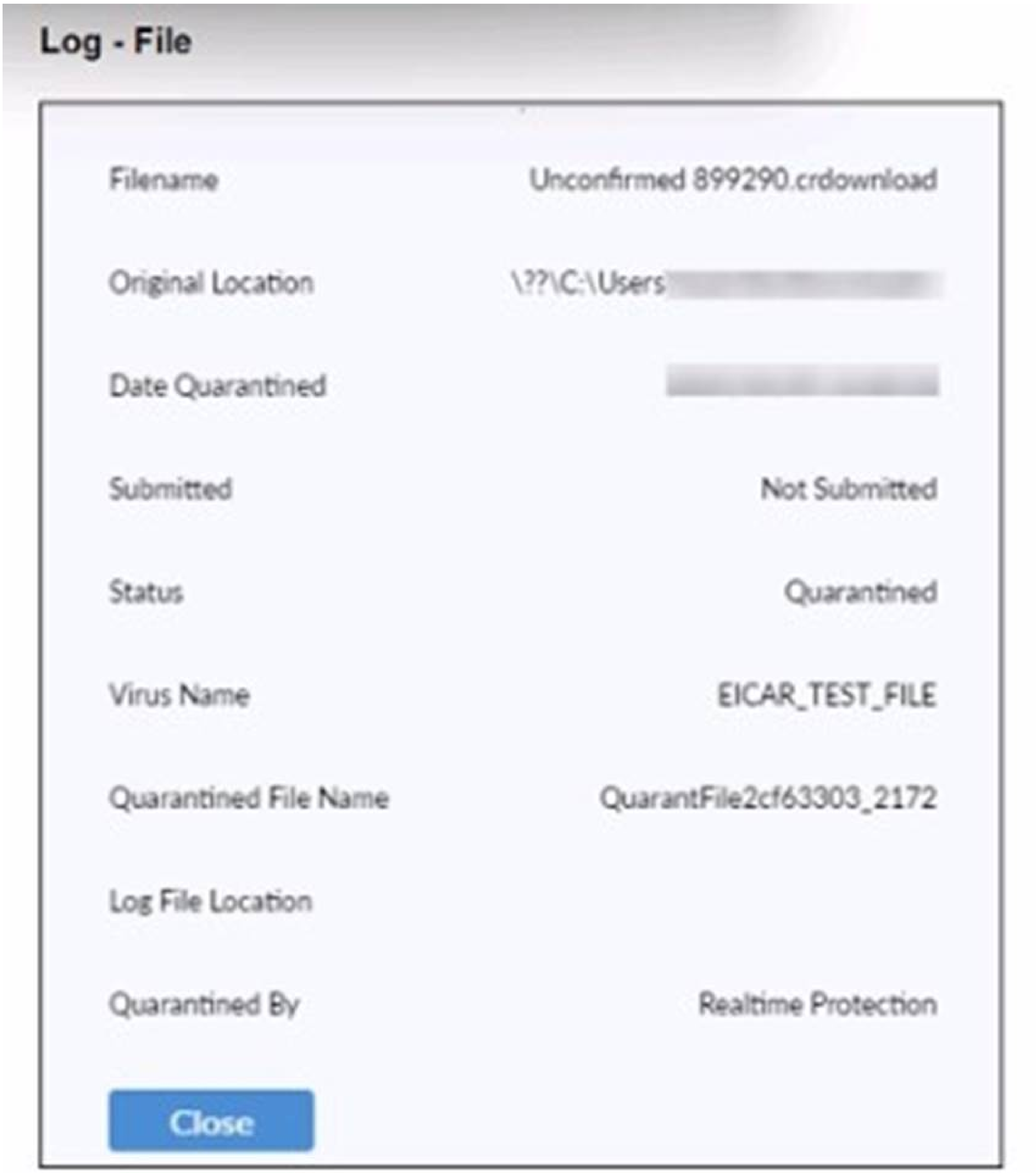
NEW QUESTION 3
Why does FortiGate need the root CA certificate of FortiCient EMS?

A. To revoke FortiClient client certificates
B. To sign FortiClient CSR requests
C. To update FortiClient client certificates
D. To trust certificates issued by FortiClient EMS

Answer: A

Explanation:
? Understanding the Need for Root CA Certificate:
? Evaluating Use Cases:
? Conclusion:
References:
? FortiClient EMS and FortiGate certificate management documentation from the study guides.

NEW QUESTION 4
Refer to the exhibit.



Log - File

Filename	Unconfirmed 899290.crdownload
Original Location	\??\C:\Users [redacted]
Date Quarantined	[redacted]
Submitted	Not Submitted
Status	Quarantined
Virus Name	EICAR_TEST_FILE
Quarantined File Name	QuarantFile2cf63303_2172
Log File Location	
Quarantined By	Realtime Protection

Based on the FortiClient tog details shown in the exhibit, which two statements ace true? (Choose two.)

A. The filename Is Unconfirmed 899290.crdovnload.
B. The file status is Quarantined
C. The filename is sent to FortiSandbox for further inspection.
D. The file location is \??\D:\Users\.

Answer: AB

NEW QUESTION 5
Which three features does FortiClient endpoint security include? (Choose three.)

A. DLP
B. Vulnerability management
C. L2TP
D. IPsec
E. Real-lime protection

Answer: BDE

Explanation:
? Understanding FortiClient Features:
? Evaluating Feature Set:
? Eliminating Incorrect Options:
References:
? FortiClient endpoint security features documentation from the study guides.

NEW QUESTION 6
Which component or device defines ZTNA lag information in the Security Fabric integration?

A. FortiClient
B. FortiGate
C. FortiClient EMS
D. FortiGate Access Proxy

Answer: C

Explanation:
? Understanding ZTNA:
? Evaluating Components:
? Conclusion:
References:
? ZTNA and FortiClient EMS configuration documentation from the study guides.

NEW QUESTION 7
Which two statements are true about ZTNA? {Choose two.)

A. ZTNA manages access for remote users only.
B. ZTNA provides role-based access.
C. ZTNA provides a security posture check.
D. ZTNA manages access through the client only.

Answer: BC

Explanation:
ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.
Two functions of ZTNA are:
ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the
device's software and hardware configurations, security settings, and the presence of malware.
ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

NEW QUESTION 8
Which two statements about ZTNA destinations are true? (Choose two.)

A. FottiClient ZTNA destinations use an existing VPN tunnel to create a secure connection.
B. FortiClient ZTNA destinations provides access through TCP forwarding.
C. FortiClient ZTNA destinations do not support a wildcard FQDN.
D. FortiClient ZTNA destination encryption is disabled by default.
E. FortiClient ZTNA destination authentication is enabled by default.

Answer: CD

NEW QUESTION 9
An administrator installs FortiClient EMS in the enterprise.
Which component is responsible for enforcing protection and checking security posture?

A. FortiClient EMS tags
B. FortiClient vulnerability scan
C. FortiClient
D. FortiClient EMS

Answer: C

Explanation:
? Understanding FortiClient EMS Components:
? Evaluating Responsibilities:
? Conclusion:
References:
? FortiClient EMS and endpoint security documentation from the study guides.

NEW QUESTION 10
What action does FortiClient anti-exploit detection take when it detects exploits?

A. Deletes the compromised application process
B. Patches the compromised application process
C. Blocks memory allocation to the compromised application process
D. Terminates the compromised application process

Answer: B

Explanation:
The anti-exploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.

NEW QUESTION 10
Which statement about FortiClient enterprise management server is true?

A. It provides centralized management of FortiGate devices.
B. lt provides centralized management of multiple endpoints running FortiClient software.
C. It provides centralized management of FortiClient Android endpoints only.
D. It provides centralized management of Chromebooks running real-time protection

Answer: B

Explanation:
FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

NEW QUESTION 12
What does FortiClient do as a fabric agent? (Choose two.)

A. Provides IOC verdicts
B. Creates dynamic policies
C. Provides application inventory
D. Automates Responses

Answer: CD

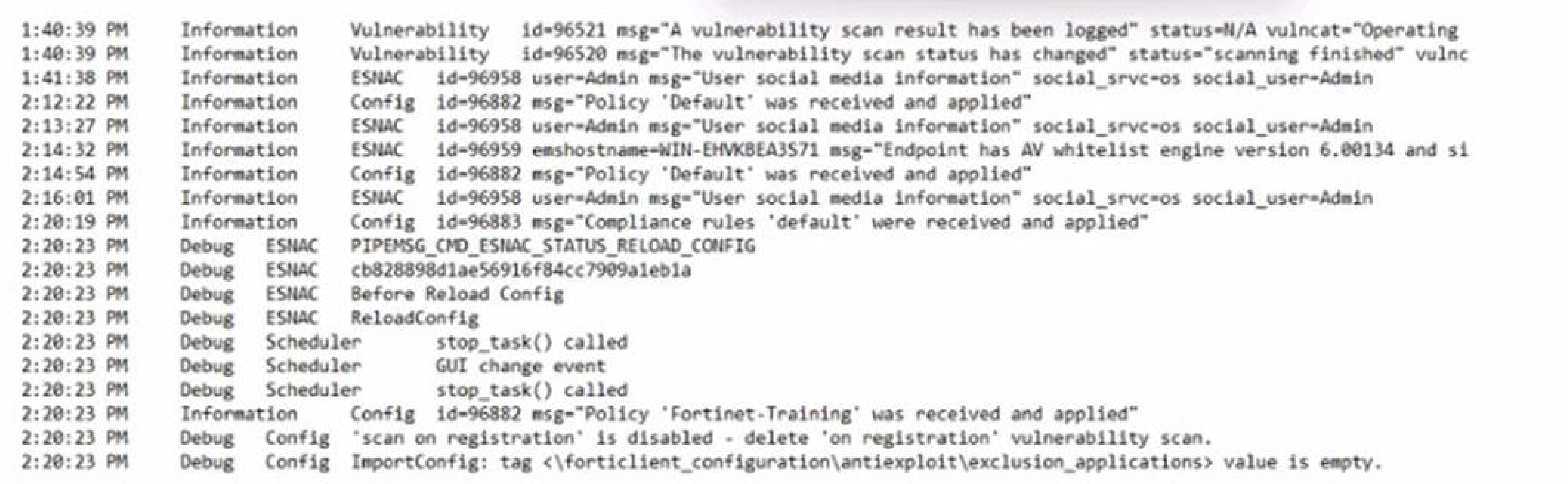
NEW QUESTION 14
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.
What could have caused this problem?

A. The FortiClient exe file is included in the distribution package
B. The FortiClient MST file is missing from the distribution package
C. FortiClient does not have permission to access the distribution package.
D. The FortiClient package is not assigned to the group

Answer: D

Explanation:
When deploying FortiClient via Microsoft AD Group Policy, it is essential to ensure that the deployment package is correctly assigned to the target group. The absence ofcustom configuration after installation can be due to several reasons, but the most likely cause is:
? Deployment Package Assignment:The FortiClient package must be assigned to
the appropriate group in Group Policy Management. If this step is missed, the installation may proceed, but the custom configurations will not be applied.
Thus, the administrator must ensure that the FortiClient package is correctly assigned to the group to include all custom configurations.
References
? FortiClient EMS 7.2 Study Guide, Deployment and Installation Section
? Fortinet Documentation on FortiClient Deployment using Microsoft AD Group Policy

NEW QUESTION 19
Exhibit.



```
1:40:39 PM    Information    Vulnerability   id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM    Information    Vulnerability   id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM    Information    ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:12:22 PM    Information    Config  id=96882 msg="Policy 'Default' was received and applied"
2:13:27 PM    Information    ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:14:32 PM    Information    ESNAC   id=96959 emshostname=WIN-EHVKBEA3S71 msg="Endpoint has AV whitelist engine version 6.00134 and si
2:14:54 PM    Information    Config  id=96882 msg="Policy 'Default' was received and applied"
2:16:01 PM    Information    ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:20:19 PM    Information    Config  id=96883 msg="Compliance rules 'default' were received and applied"
2:20:23 PM    Debug   ESNAC   PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
2:20:23 PM    Debug   ESNAC   cb828898d1ae56916f84cc7909a1eb1a
2:20:23 PM    Debug   ESNAC   Before Reload Config
2:20:23 PM    Debug   ESNAC   ReloadConfig
2:20:23 PM    Debug   Scheduler       stop_task() called
2:20:23 PM    Debug   Scheduler       GUI change event
2:20:23 PM    Debug   Scheduler       stop_task() called
2:20:23 PM    Information    Config  id=96882 msg="Policy 'Fortinet-Training' was received and applied"
2:20:23 PM    Debug   Config  'scan on registration' is disabled - delete 'on registration' vulnerability scan.
2:20:23 PM    Debug   Config  ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.
```

Based on the FortiClient logs shown in the exhibit, which endpoint profile policy is currently applied lo the ForliClient endpoint from the EMS server?

A. Fortinet-Training
B. Default configuration policy c
C. Compliance rules default
D. Default

Answer: A

Explanation:
? Observation of Logs:
? Evaluating Policies:
? Conclusion:
References:
? FortiClient EMS policy configuration and log analysis documentation from the study guides.

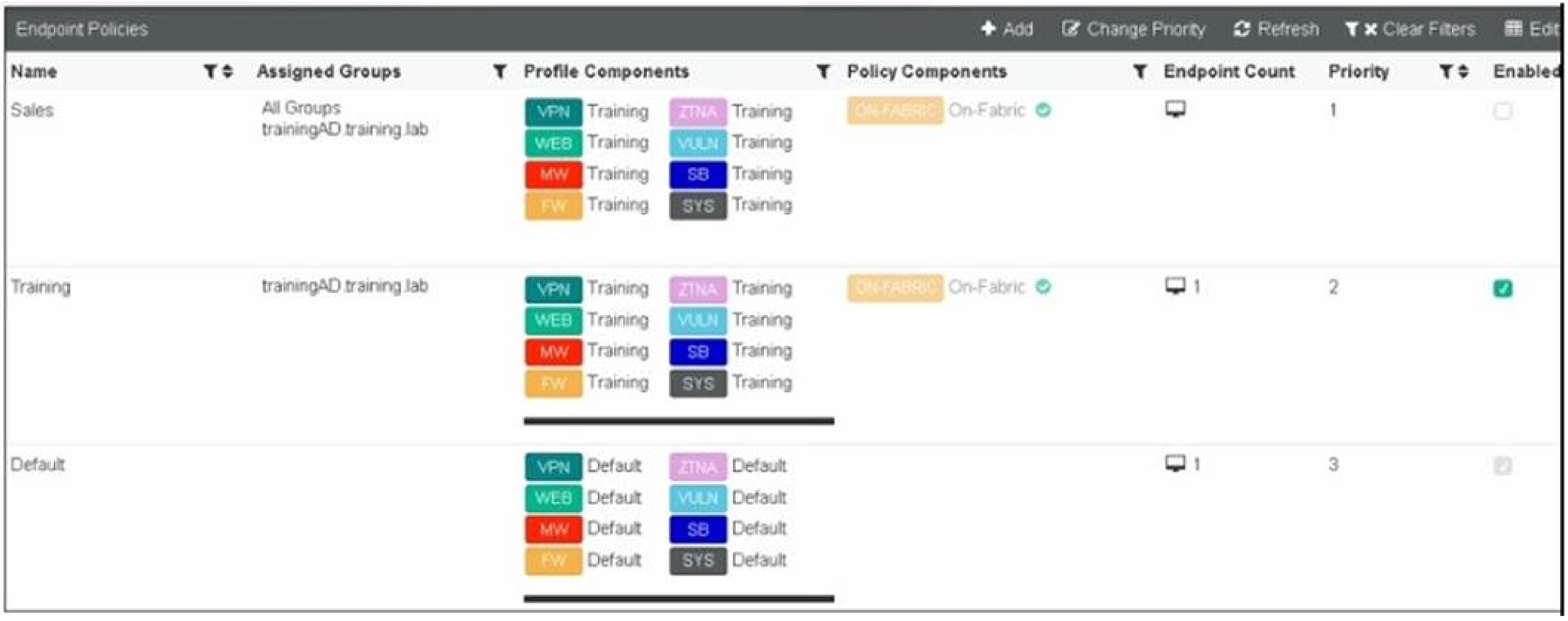
NEW QUESTION 23
An administrator installs FortiClient on Windows Server. What is the default behavior of real-time protection control?

A. Real-time protection must update AV signature database
B. Real-time protection sends malicious files to FortiSandbox when the file is not detected locally
C. Real-time protection is disabled
D. Real-time protection must update the signature database from FortiSandbox

Answer: C

Explanation:
When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:
? Real-time protection is disabled:By default, FortiClient does not enable real-time
protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints.
Thus, real-time protection is disabled by default on Windows Server installations.
References
? FortiClient EMS 7.2 Study Guide, Real-time Protection Section
? Fortinet Documentation on FortiClient Default Settings for Server Installations

NEW QUESTION 24
FortiClient EMS endpoint policies



Name	Assigned Groups	Profile Components	Policy Components	Endpoint Count	Priority	Enabled
Sales	All Groups trainingAD.training.lab	VPN Training ZTNA Training WEB Training VULN Training MW Training SB Training FW Training SYS Training	ON-FABRIC On-Fabric ✓		1	□
Training	trainingAD.training.lab	VPN Training ZTNA Training WEB Training VULN Training MW Training SB Training FW Training SYS Training	ON-FABRIC On-Fabric ✓	1	2	☑
Default		VPN Default ZTNA Default WEB Default VULN Default MW Default SB Default FW Default SYS Default		1	3	☑

Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

A. The Training policy
B. Both the Sales and Training policies because their priority is higher than the Default policy
C. The Default policy because it has the highest priority
D. The sales policy

Answer: A

Explanation:
? Observation of Endpoint Policies:
? Evaluating Policy Assignment:
? Conclusion:
References:
? FortiClient EMS policy configuration and priority management documentation from the study guides.

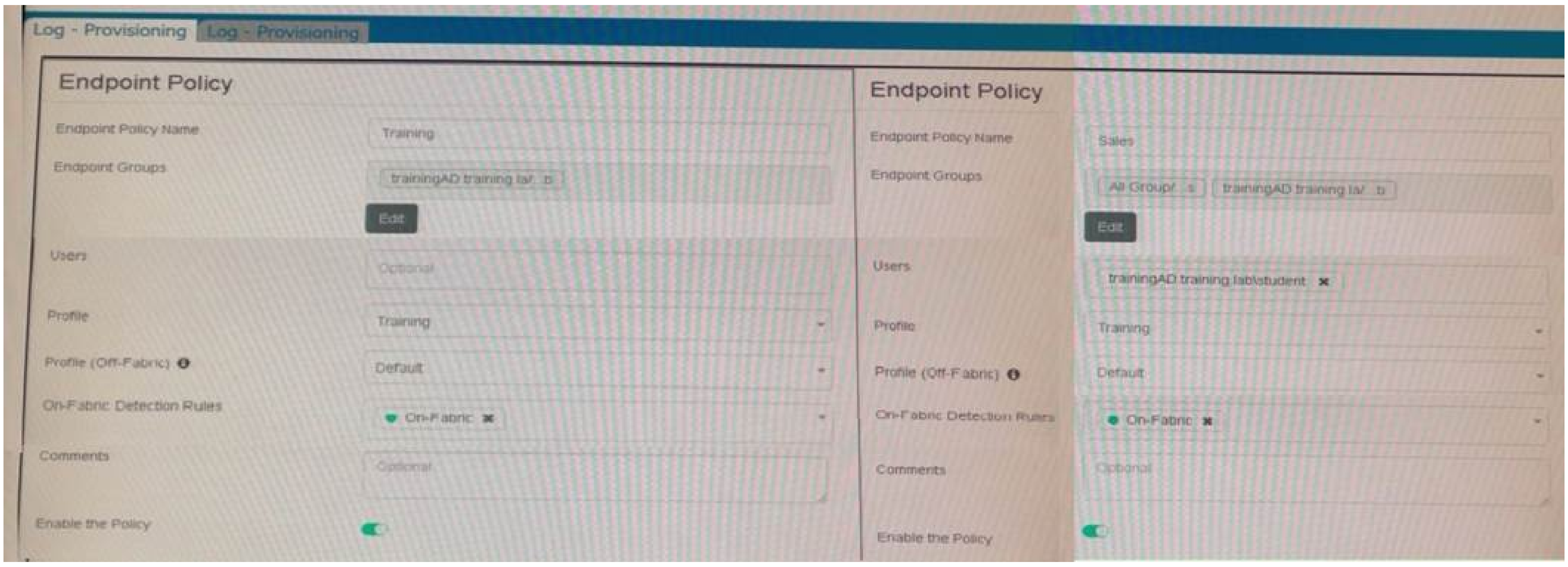
NEW QUESTION 28
Which component or device shares ZTNA tag information through Security Fabric integration?

A. FortiGate
B. FortiGate Access Proxy
C. FortiClient

Answer: A

Explanation:
FortiClient EMS is the component that shares ZTNA tag information through Security Fabric integration. ZTNA tags are synchronized from FortiClient EMS as inputs for the FortiGate application gateway. They can be used in ZTNA policies as security posture checks to ensure certain security criteria are met. FortiClient EMS can share ZTNA tags across multiple devices in the Fabric, such as FortiGate, FortiManager, and FortiAnalyzer. FortiClient EMS can also share ZTNA tags across multiple VDOMs on thesame FortiGate device. FortiClient EMS can be configured to control the ZTNA tag sharing behavior in the Fabric Devices settings1.
FortiGate is the device that enforces ZTNA policies using ZTNA tags. FortiGate can receive ZTNA tags from FortiClient EMS via Fabric Connector. FortiGate can also publish ZTNA services through the ZTNA portal, which allows users to access applications without installing FortiClient. FortiGate can also provide ZTNA inline CASB for SaaS application access control2.
FortiGate Access Proxy is a feature that enables FortiGate to act as a proxy for ZTNA traffic. FortiGate Access Proxy can be deployed in front of the application servers to provide ZTNA protection. FortiGate Access Proxy can also be deployed behind the application servers to provide ZTNA visibility. FortiGate Access Proxy can use ZTNA tags to identify and authenticate users and devices2.
FortiClient is the endpoint software that connects to ZTNA services. FortiClient can register ZTNA tags with FortiClient EMS based on the endpoint security posture. FortiClient can also use ZTNA tags to access ZTNA services published by FortiGate. FortiClient can also use ZTNA tags to access SaaS applications with ZTNA inline CASB2.
References :=
? Technical Tip: Behavior of ZTNA Tags shared across multiple vdoms or multiple FortiGate firewalls in the Security Fabric connected to the same FortiClient EMS Server
? Synchronizing FortiClient ZTNA tags
? Zero Trust Network Access (ZTNA) to Control Application Access

NEW QUESTION 30
Refer to the exhibits.

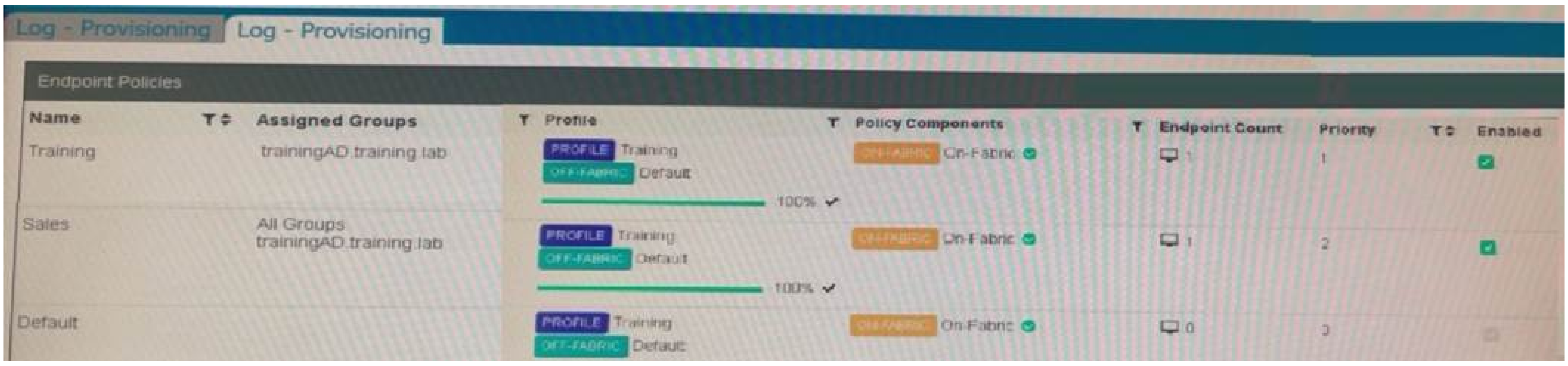


Endpoint Policy

Endpoint Policy Name	Training
Endpoint Groups	trainingAD.training.la/ b
Users	Optional
Profile	Training
Profile (Off-Fabric)	Default
On-Fabric Detection Rules	On-Fabric ✕
Comments	Optional
Enable the Policy	●

Endpoint Policy

Endpoint Policy Name	Sales
Endpoint Groups	All Groups/ s trainingAD.training.la/ b
Users	trainingAD.training.lab\student ✕
Profile	Training
Profile (Off-Fabric)	Default
On-Fabric Detection Rules	On-Fabric ✕
Comments	Optional
Enable the Policy	●



Endpoint Policies

Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Priority	Enabled
Training	trainingAD.training.lab	PROFILE Training OFF-FABRIC Default 100% ✓	ON-FABRIC On-Fabric ✓	1	1	☑
Sales	All Groups trainingAD.training.lab	PROFILE Training OFF-FABRIC Default 100% ✓	ON-FABRIC On-Fabric ✓	1	2	☑
Default		PROFILE Training OFF-FABRIC Default	ON-FABRIC On-Fabric ✓	0	3	□

Which shows the configuration of endpoint policies.

Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

A. FortiClient EMS will assign the Sales policy
B. FortiClient EMS will assign the Training policy
C. FortiClient EMS will assign the Default policy
D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Answer: B

Explanation:
Based on the configuration shown in the exhibits:
? There are three endpoint policies configured: Training, Sales, and Default.
? The "Training" policy is assigned to the "trainingAD.training.lab" group.
? The "Sales" policy is assigned to "All Groups" and "trainingAD.training.lab/student."
? The "Default" policy has no specific groups assigned.
When someone logs in with the user account "student" on an endpoint in the "trainingAD" domain:
? The "Training" policy is specifically assigned to the "trainingAD.training.lab" group.
? The "Sales" policy includes "trainingAD.training.lab/student" but not the general "trainingAD.training.lab" group.
? The system will prioritize the most specific match for the group.
Therefore, FortiClient EMS will assign the "Training" policy to the "student" account logging into the "trainingAD" domain as it matches the group "trainingAD.training.lab" directly. References
? FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section
? FortiClient EMS Documentation on Group Policy Assignment and Matching

NEW QUESTION 32
Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

A. L2TP
B. PPTP
C. IPSec
D. SSL VPN

Answer: CD

Explanation:
FortiClient supports initiating the following VPN types from the Windows command prompt:
? IPSec VPN:FortiClient can establish IPSec VPN connections using command line
instructions.
? SSL VPN:FortiClient also supports initiating SSL VPN connections from the Windows command prompt.
These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.
References
? FortiClient EMS 7.2 Study Guide, VPN Configuration Section
? Fortinet Documentation on Command Line Options for FortiClient VPN

NEW QUESTION 35
Which statement about FortiClient comprehensive endpoint protection is true?

A. It helps to safeguard systems from email spam
B. It helps to safeguard systems from data loss.
C. It helps to safeguard systems from DDoS.
D. It helps to safeguard systems from advanced security threats, such as malware.

Answer: D

Explanation:
FortiClient provides comprehensive endpoint protection for your Windows- based, Mac-based, and Linuxbased desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

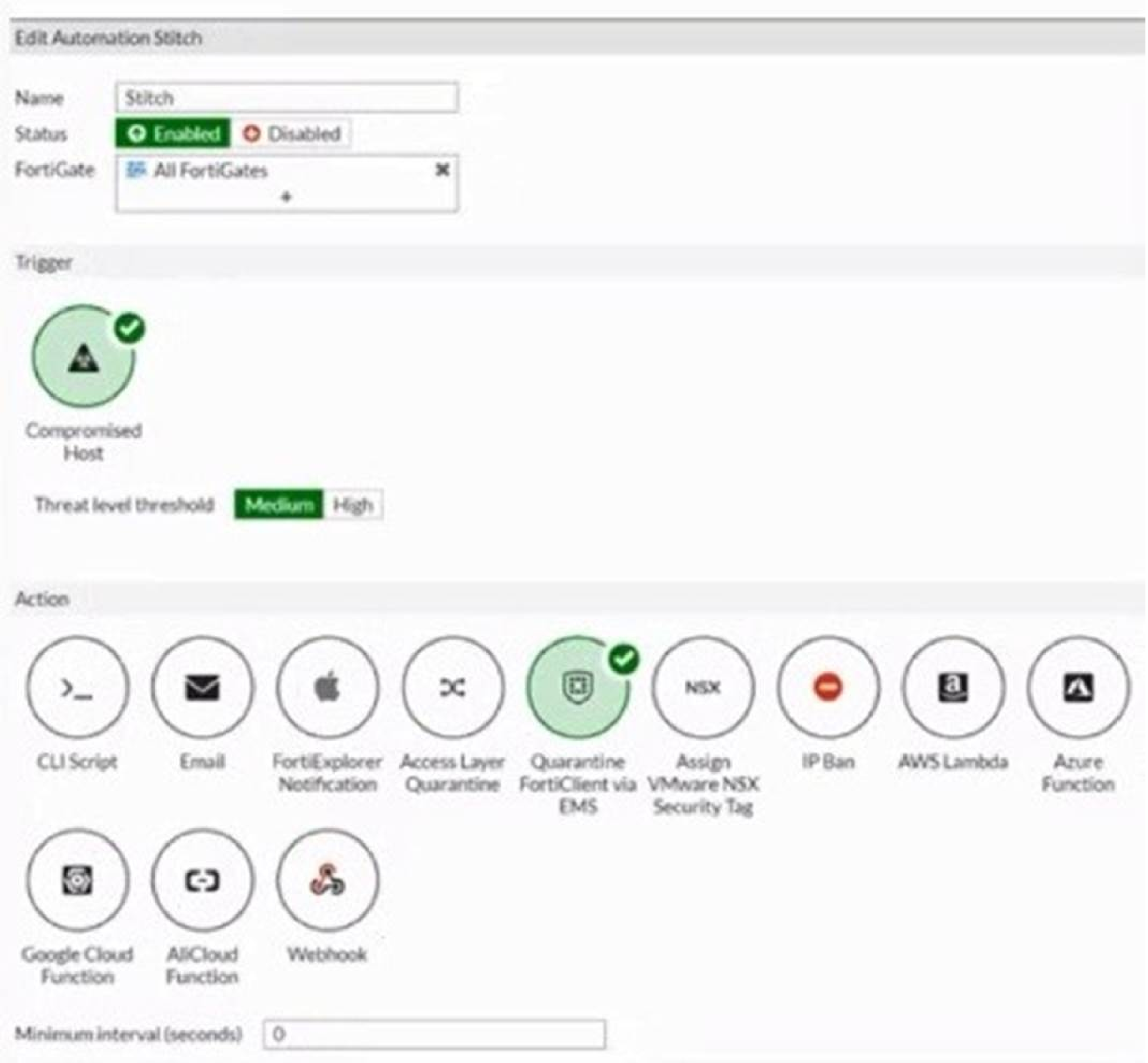
NEW QUESTION 38
Which three types of antivirus scans are available on FortiClient? (Choose three)

A. Proxy scan
B. Full scan
C. Custom scan
D. Flow scan
E. Quick scan

Answer: BCE

Explanation:
FortiClient offers several types of antivirus scans to ensure comprehensive protection:
? Full scan:Scans the entire system for malware, including all files and directories.
? Custom scan:Allows the user to specify particular files, directories, or drives to be scanned.
? Quick scan:Scans the most commonly infected areas of the system, providing a faster scanning option.
These three types of scans provide flexibility and thoroughness in detecting and managing malware threats.
References
? FortiClient EMS 7.2 Study Guide, Antivirus Scanning Options Section
? Fortinet Documentation on Types of Antivirus Scans in FortiClient

NEW QUESTION 41
Refer to the exhibit.


Edit Automation Stitch

Name: Stitch
Status: Enabled | Disabled
FortiGate: All FortiGates

Trigger

Compromised Host

Threat level threshold: Medium | High

Action

Minimum interval (seconds): 0

Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

A. Endpoints will be quarantined through EMS
B. Endpoints will be banned on FortiGate
C. An email notification will be sent for compromised endpoints
D. Endpoints will be quarantined through FortiSwitch

Answer: A

Explanation:
Based on the Security Fabric automation settings shown in the exhibit:
? The automation stitch is configured with a trigger for a "Compromised Host."
? The action specified for this trigger is "Quarantine FortiClient via EMS."
? This indicates that when an endpoint is detected as compromised, FortiClient EMS will quarantine the endpoint as part of the automation process.
Therefore, the action taken on compromised endpoints will be to quarantine them through EMS.
References
? FortiGate Security 7.2 Study Guide, Automation Stitches and Actions Section
? Fortinet Documentation on Configuring Automation Stitches and Quarantine Actions

NEW QUESTION 46
......