ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

When an administrator creates a deployment profile on FortiClient EMS. which statement about the deployment profile is true?

A. Deployment-2 will upgrade FortiClient on both the AD group and workgroup.

B. Deployment-1 will install FortiClient on new AO group endpoints.

C. Deployment-2 will install FortiClient on both the AD group and workgroup.

D. Deployment-1 will upgrade FortiClient only on the workgroup.

Answer: A

Explanation:

Deployment Profiles Analysis:

Deployment-1 has the "First-Time-Installation" package and is assigned to "All Groups" with a priority of 1 but is not enabled.

Deployment-2 has the "To-Upgrade" package, is assigned to both "All Groups" and "trainingAD.training.lab," with a priority of 2 and is enabled.

Evaluating Deployment-2:

Deployment-2 will upgrade FortiClient on both "All Groups" and "trainingAD.training.lab" since it is enabled and assigned to these groups. This includes both AD (Active Directory) groups and workgroups.

Conclusion:

Since Deployment-2 is set to upgrade FortiClient on all the assigned groups and workgroups, the correct answer is A.

Reference:

FortiClient EMS deployment and profile documentation from the study guides.

Question: 2

Exhibit.

Based on the logs shown in the exhibit, why did FortiClient EMS tail to install FortiClient on the endpoint?

A. The FortiClient antivirus service is not running.

B. The Windows installer service is not running.

C. The remote registry service is not running.

D. The task scheduler service is not running.

Answer: D

Explanation:

https://community.fortinet.com/t5/FortiClient/Technical-Note-FortiClient-fails-to-install-from- FortiClient-EMS/ta-p/193680

The deployment service error message may be caused by any of the following. Try eliminating them all, one at a time.

1. Wrong username or password in the EMS profile
2. Endpoint is unreachable over the network
3. Task Scheduler service is not running
4. Remote Registry service is not running
5. Windows firewall is blocking connection

Question: 3

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: B, C

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.

Question: 4

When site categories are disabled in FortiClient web filter, which feature can be used to protect the endpoint from malicious web access?

A. Real-time protection list

B. Block malicious websites on antivirus

C. FortiSandbox URL list

D. Web exclusion list

Answer: D

Explanation:

Web Filter Functionality:

When site categories are disabled in the FortiClient web filter, the endpoint still requires protection from malicious web access.

Alternative Protection Features:

The web exclusion list can be used to manage and block specific URLs that are known to be malicious, providing a way to control and secure web access even without site categories being enabled.

Conclusion:

The correct feature that can be used to protect the endpoint in this scenario is the web exclusion list (D).

Reference:

FortiClient web filter configuration and features from the study guides.

Question: 5

Exhibit.

FortiClient Status - GUI

Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status.

Remote-Client is tagged as Remote-User* on the FortiClient EMS Zero Trust Tag Monitor.

What must an administrator do to show the tag on the FortiClient GUI?

A. Change the FortiClient EMS shared settings to enable tag visibility.

B. Change the endpoint alerts configuration to enable tag visibility.

C. Update tagging rule logic to enable tag visibility.

D. Change the FortiClient system settings to enable lag visibility.

Answer: B

Explanation:

Observation of Exhibits:

The exhibits show the Zero Trust Tag Monitor on FortiClient EMS and the FortiClient GUI status.

Remote-Client is tagged as "Remote-Endpoints" on the FortiClient EMS Zero Trust Tag Monitor.

Enabling Tag Visibility:

To show the tag on the FortiClient GUI, the endpoint alerts configuration must be adjusted to enable tag visibility.

Verification:

The correct action is to change the endpoint alerts configuration to enable tag visibility, ensuring that the tag appears in the FortiClient GUI.

Reference:

FortiClient EMS and FortiClient configuration documentation from the study guides.

Question: 6

An administrator wants to simplify remote access without asking users to provide user credentials Which access control method provides this solution?

A. ZTNA full mode

B. SSL VPN

C. L2TP

D. ZTNA IP/MAC littering mode

Answer: A

Explanation:

Simplifying Remote Access:

The administrator wants to simplify remote access without asking users to provide user credentials.

Evaluating Access Control Methods:

ZTNA full mode can provide seamless access by leveraging device identity and posture, eliminating the need for user credentials for each access request.

Other methods like SSL VPN and L2TP typically require user credentials.

Conclusion:

The correct access control method that provides this solution is ZTNA full mode.

Reference:

ZTNA section in the FortiGate Infrastructure 7.2 Study Guide.

Question: 7

A FortiClient EMS administrator has enabled the compliance rule for the sales department Which Fortinet device will enforce compliance with dynamic access control?

A. FortiClient

B. FortiClient EMS

C. FortiGate

D. FortiAnalyzer

Answer: C

Explanation:

Understanding Compliance Rules:

The compliance rule for the sales department needs to be enforced dynamically.

Enforcing Compliance:

FortiGate is responsible for enforcing compliance by integrating with FortiClient EMS to apply dynamic access control based on compliance status.

Conclusion:

The Fortinet device that will enforce compliance with dynamic access control is the FortiGate.

Reference:

Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

Question: 8

In a ForliSandbox integration, what does the remediation option do?

A. Deny access to a tile when it sees no results

B. Alert and notify only

C. Exclude specified files

D. Wait for FortiSandbox results before allowing files

Answer: B

Explanation:

Understanding FortiSandbox Integration:

In a FortiSandbox integration, various remediation options are available for handling suspicious files.

Evaluating Remediation Options:

The remediation option for alerting and notifying without blocking access or waiting for results is essential to understand.

Conclusion:

The correct action for the remediation option in this context is to alert and notify only.

Reference:

FortiSandbox integration documentation from the study guides.

Question: 9

An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate What is the prerequisite to get FortiClient EMS lo connect to FortiGate successfully?

A. Import and verify the FortiClient EMS tool CA certificate on FortiGate.

B. Revoke and update the FortiClient client certificate on EMS.

C. Import and verify the FortiClient client certificate on FortiGate.

D. Revoke and update the FortiClient EMS root CA.

Answer: A

Explanation:

Connecting FortiClient EMS to FortiGate:

The administrator needs to establish a connection between FortiClient EMS and FortiGate as a fabric connector.

Prerequisites for Connection:

A key prerequisite is the import and verification of the FortiClient EMS tool CA certificate on FortiGate to ensure a trusted connection.

Conclusion:

The correct prerequisite for a successful connection is to import and verify the FortiClient EMS tool CA certificate on FortiGate.

Reference:

FortiClient EMS and FortiGate connection and certificate management documentation from the study guides.

Question: 10

An administrator must add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.

Which solution can provide secure access between FortiClient EMS and the Active Directory server?

A. Configure and deploy a FortiGate device between FortiClient EMS and the Active Directory server.

B. Configure Active Directory and install FortiClient EMS on the same VM.

C. Configure a slave FortiClient EMS on a virtual machine.

D. Configure an Active Directory connector between FortiClient EMS and the Active Directory server.

Answer: A

Explanation:

Requirement:

The administrator needs to add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.

Solution Analysis:

The goal is to securely connect FortiClient EMS and the Active Directory server despite being in different security zones.

Evaluating Options:

Installing FortiClient EMS on the same VM as Active Directory (option B) is not practical due to security zone separation.

Configuring a slave FortiClient EMS on a virtual machine (option C) does not address the need for secure communication.

Configuring an Active Directory connector (option D) may not be sufficient without secure routing.

Conclusion:

Deploying a FortiGate device between FortiClient EMS and the Active Directory server ensures secure and controlled access between the two zones.

Reference:

FortiClient EMS and FortiGate configuration and deployment documentation from the study guides.

Question: 11

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

Explanation:

Question: 12

Exhibit.

```
1:46:59 PM  Information  Vulnerability .  id-96521 msg^A vulnerability scan result has been logged" status-H/A vulncat-"Operating
1:4639 PM   Information  Vulnerability .  id-96528 msg»"The vulnerability scan status has changed" status-"scannlng finished" vulnc
1:41:38 PM  Information  ESHAC  id-96958  user-Admin msg-"User social media information" social_srvc-os social.user-Admin
2:12:22 PM  Information  Config  id-%882   msg-"Pollcy 'Default* was received and applied"
2:13:27 PM  Information  ESHAC  ld-%958   user-Admin msg-"User social media information" soclal_srvc-©s socialuser-Admin
2:14:32 PM  Information  ESHAC  id-96959  emsbostoame-HIN-EHVK9EAJS71 msg-"Endpoint has AV whitelist engine version 6.86134 and si
2:14:54 PM  Information  Config  id-9688?  msg-'Policy 'Default* was received and applied"
2:16:81 PM  Information  ESHAC  ld-%958   user-Admin msg-"User social media information" socleisrvc-os soclal_user-Admin
2:2819 PM   Information  Config  id-96883  msg-"Compliance rules 'default* were received and applied"

Debug ESHAC  2:28:23 PM  PIPEMMJMDJSNMJTATUSRflOADJWK
Debug        2:28:23 PM      ESHAC      cb82B898dlae56916f84cc 7909a lebla
Debug        2:28:23 PM      ESHAC      Before Reload Config
Debug        2:28:23 PM      ESHAC      ReloadConfig
Debug        2:28:23 PM      Scheduler  stop_task() called
Debug        2:28:23 PM      Scheduler  GUI change event
Debug        2:28:23 PM      Scheduler  stop.task() called
Information  2:28:23 PM  Config id-96882 msg-"Policy 'Fortiiwt-Training* was received and applied"
Debug Config 2:28:23 PM  'scan on registration* is disabled - delete 'on registration* vulnerability scan.
Debug Config 2:28:23 PM  lnoortConfjg: tag <\fortlclient_configuration\antiexploit\exclusion_8pplicatlor$> value is empty.
             2:28:23 PM
             2:28:23 PM
```

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:

The logs show a policy named "Fortinet-Training" being applied to the endpoint.

Evaluating Policies:

The log entries indicate that the "Fortinet-Training" policy was received and applied.

Conclusion:

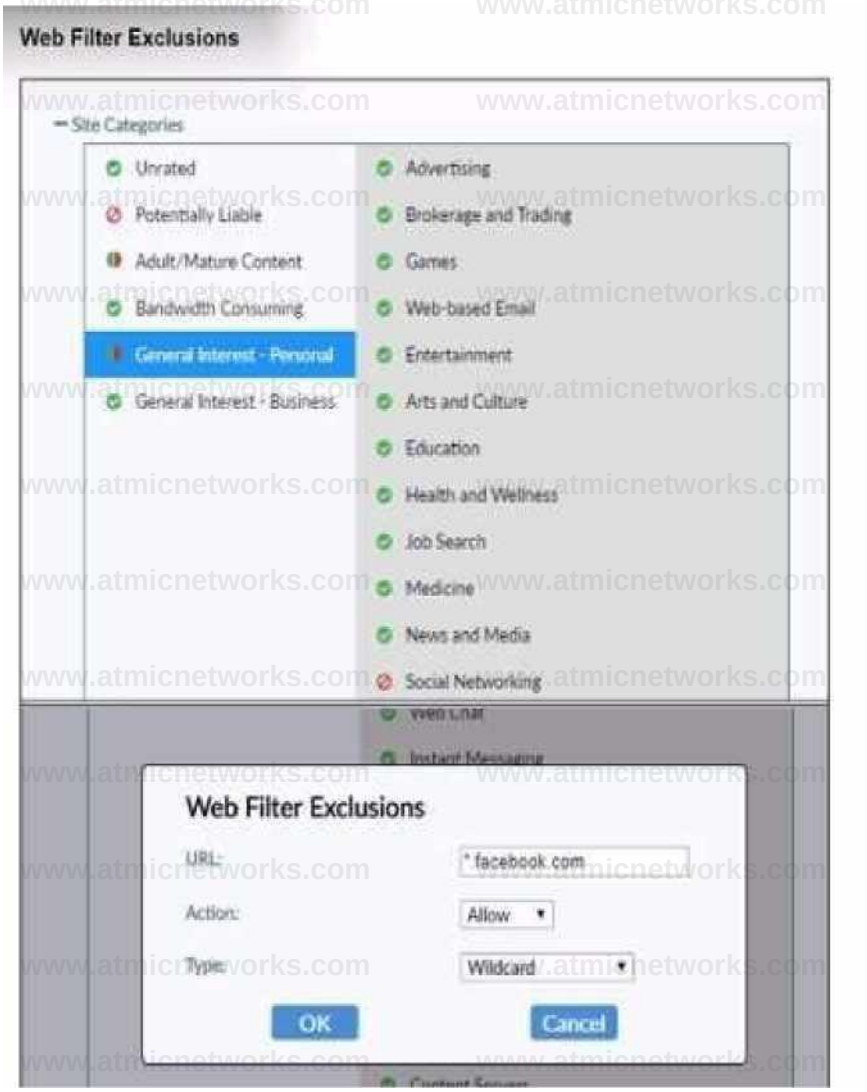
Based on the logs, the currently applied policy on the FortiClient endpoint is "Fortinet-Training".

Reference:

FortiClient EMS policy configuration and log analysis documentation from the study guides.

Question: 13

Refer to the exhibit.



Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www facebook com?

A. FortiClient will allow access to Facebook.

B. FortiClient will block access to Facebook and its subdomains.

C. FortiClient will monitor only the user's web access to the Facebook website

D. FortiClient will prompt a warning message to want the user before they can access the Facebook website

Answer: B

Explanation:

Observation of Web Filter Exclusions:

The exhibit shows a web filter exclusion for "*.facebook.com" with the action set to "Allow."

Evaluating Actions:

This configuration means that FortiClient will allow access to Facebook and its subdomains.

Conclusion:

When users try to access "www.facebook.com," FortiClient will allow the access based on the web filter exclusion settings.

Reference:

FortiClient web filter configuration and exclusion documentation from the study guides.

Question: 14

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:

The root CA certificate of FortiClient EMS is necessary for FortiGate to trust certificates issued by FortiClient EMS.

Evaluating Use Cases:

FortiGate needs the root CA certificate to establish trust and validate certificates issued by FortiClient EMS.

Conclusion:

The primary reason FortiGate needs the root CA certificate of FortiClient EMS is to trust certificates issued by FortiClient EMS.

Reference:

FortiClient EMS and FortiGate certificate management documentation from the study guides.

Question: 15

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:

FortiClient endpoint security includes several features aimed at protecting and managing endpoints.

Evaluating Feature Set:

Vulnerability management is a key feature of FortiClient, helping to identify and address vulnerabilities (B).

IPsec is supported for secure VPN connections (D).

Real-time protection is crucial for detecting and preventing threats in real-time (E).

Eliminating Incorrect Options:

Data Loss Prevention (DLP) (A) is typically managed by FortiGate or FortiMail.

L2TP (C) is a protocol used for VPNs but is not specifically a feature of FortiClient endpoint security.

Reference:

FortiClient endpoint security features documentation from the study guides.

Question: 16

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:

Zero Trust Network Access (ZTNA) requires defining tags for identifying and managing endpoint access.

Evaluating Components:

FortiClient EMS is responsible for managing and defining ZTNA tag information within the Security Fabric.

Conclusion:

The correct component that defines ZTNA tag information in the Security Fabric integration is FortiClient EMS.

Reference:

ZTNA and FortiClient EMS configuration documentation from the study guides.

Question: 17

Which security fabric component sends a notification io quarantine an endpoint after IOC detection "n the automation process?

A. FortiAnalyzer

B. FortiGate

C. FortiClient EMS

D. FortiClient

Answer: C

Explanation:

Understanding the Automation Process:

In the Security Fabric, automation processes can include actions such as quarantining an endpoint after an IOC (Indicator of Compromise) detection.

Evaluating Responsibilities:

FortiClient EMS plays a crucial role in endpoint management and can send notifications to quarantine endpoints.

Conclusion:

The correct security fabric component that sends a notification to quarantine an endpoint after IOC detection is FortiClient EMS.

Reference:

FortiClient EMS and automation process documentation from the study guides.

Question: 18

An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?

A. It redirects the client request to the access proxy.

B. It uses the access proxy.

C. It defines ZTNA server.

D. It only uses ZTNA tags to control access for endpoints.

Answer: A

Explanation:

"The firewall policy matches and redirects client requests to the access proxy VIP"
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration

Question: 19

Refer to the exhibit.

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

Explanation:

Question: 20

Which two are benefits of using multi-tenancy mode on FortiClient EMS? (Choose two.)

A. Separate host servers manage each site.

B. Licenses are shared among sites

C. The fabric connector must use an IP address to connect to FortiClient EMS.

D. It provides granular access and segmentation.

Answer: C, D

Explanation:

Understanding Multi-Tenancy Mode:

Multi-tenancy mode allows multiple independent sites or tenants to be managed from a single FortiClient EMS instance.

Evaluating Benefits:

Licenses can be shared among sites, making it cost-effective (B).

It provides granular access and segmentation, allowing for detailed control and separation between tenants (D).

Eliminating Incorrect Options:

Separate host servers managing each site (A) is not a feature of multi-tenancy mode.

The fabric connector's use of an IP address (C) is unrelated to multi-tenancy benefits.

Reference:

FortiClient EMS multi-tenancy configuration and benefits documentation from the study guides.

Question: 21

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:

FortiClient EMS manages and configures endpoint security settings, while FortiClient installed on the endpoint enforces protection and checks security posture.

Evaluating Responsibilities:

FortiClient performs the actual enforcement of security policies and checks the security posture of the endpoint.

Conclusion:

The component responsible for enforcing protection and checking security posture is FortiClient (C).

Reference:

FortiClient EMS and endpoint security documentation from the study guides.

Question: 22

Refer to the exhibit.

Based on The settings shown in The exhibit, which statement about FortiClient behaviour is Hue?

A. FortiClient scans infected files when the user copies files to the Resources folder.

B. FortiClient quarantines infected ties and reviews later, after scanning them.

C. FortiClient copies infected files to the Resources folder without scanning them.

D. FortiClient blocks and deletes infected files after scanning them.

Answer: A

Explanation:

Based on the settings shown in the exhibit, FortiClient is configured to scan files as they are downloaded or copied to the system. This means that if a user copies files to the “Resources” folder, which is not listed under exclusions, FortiClient will scan these files for infections. The exclusion path mentioned in the settings, "C:\Users\Administrator\Desktop\Resources", indicates that any files copied to this specific folder will not be scanned, but since the question implies that the “Resources” folder is not the same as the excluded path, FortiClient will indeed scan the files for infections.

Question: 23

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.

Question: 24

What is the function of the quick scan option on FortiClient?

A. It scans programs and drivers that are currently running, for threats

B. It performs a full system scan including all files, executable files. DLLs, and drivers for throats.

C. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.

D. It scans executable files. DLLs, and drivers that are currently running, for threats.

Answer: B

Explanation:

Understanding Quick Scan Function:

The quick scan option on FortiClient is designed to scan certain elements of the system quickly for

threats.

Evaluating Scan Scope:

The quick scan specifically targets executable files, DLLs, and drivers that are currently running, providing a rapid assessment of the active components of the system.

Conclusion:

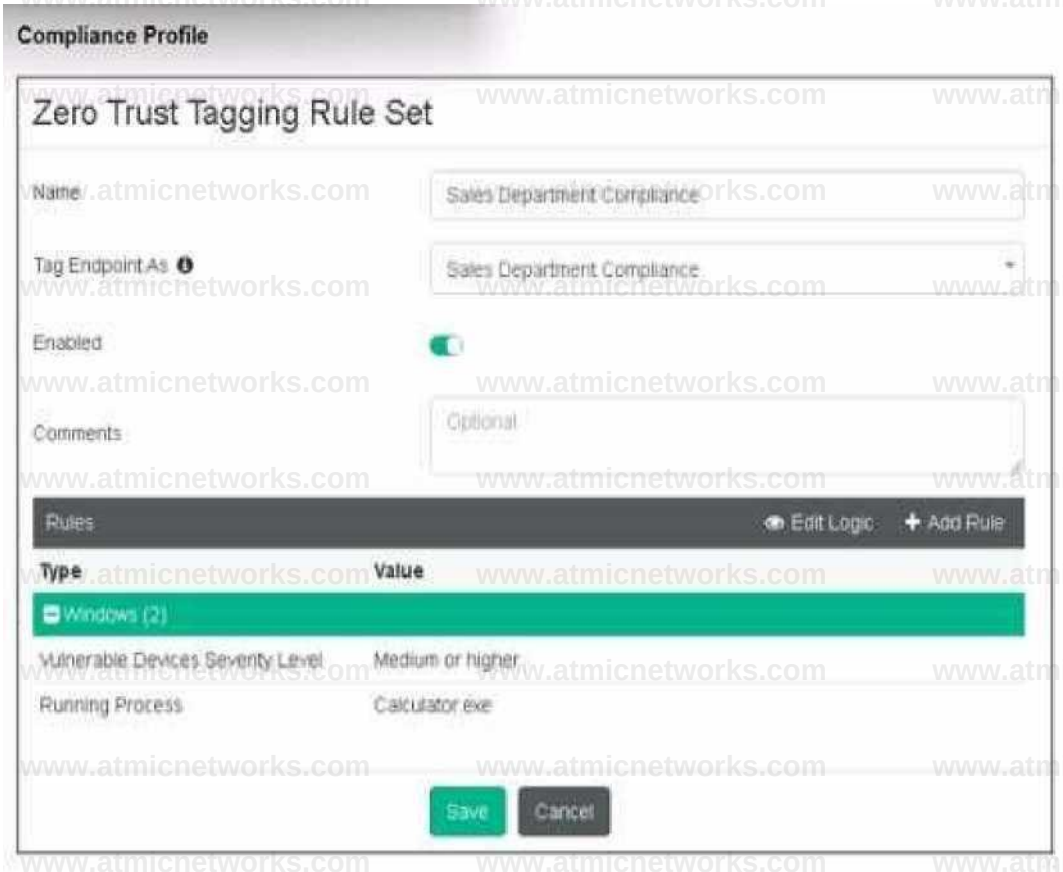
The correct answer is D, as it accurately describes the function of the quick scan option on FortiClient.

Reference:

FortiClient scanning options documentation from the study guides.

Question: 25

Refer to the exhibit.



Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

A. Enable the web filter profile.

B. Run Calculator application on the endpoint.

C. Integrate FortiSandbox tor infected file analysis

D. Patch applications that have vulnerability rated as high or above.

Answer: BD

Explanation:

Observation of Compliance Profile:

The compliance profile shown in the exhibit includes rules for vulnerability severity level and running process (Calculator.exe).

Evaluating Actions for Compliance:

To make the endpoint compliant, the administrator needs to ensure that the vulnerability severity level is medium or higher is patched (D).

Additionally, the Calculator.exe application must be running on the endpoint (B).

Eliminating Incorrect Options:

Enabling the web filter profile (A) is not related to the compliance rules shown.

Integrating FortiSandbox (C) is not a requirement in the given compliance profile.

Conclusion:

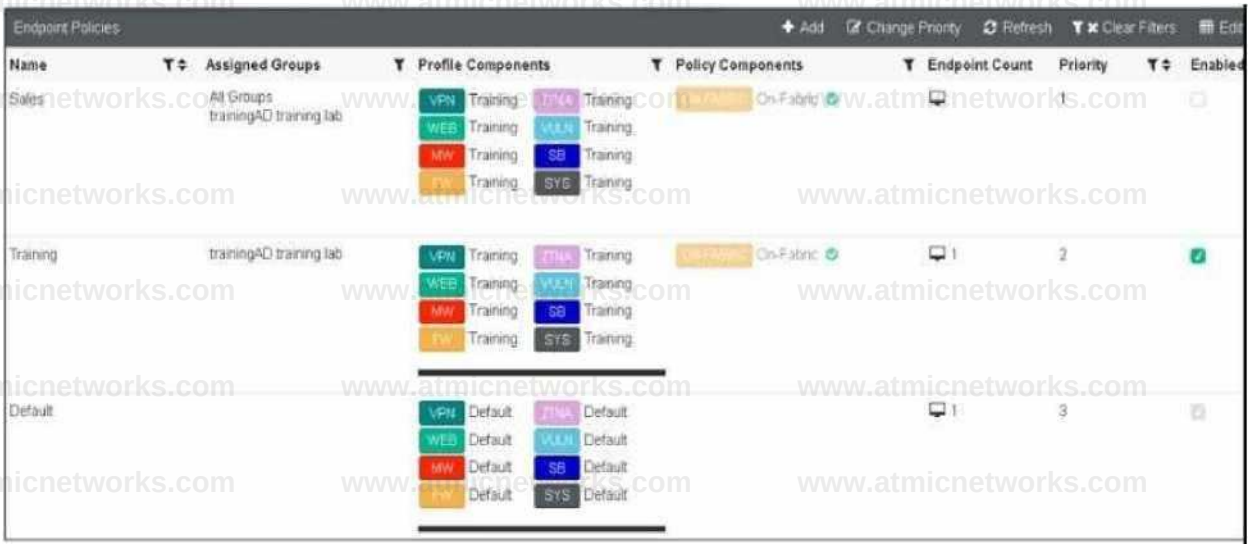
The correct actions are to run the Calculator application on the endpoint (B) and patch applications with vulnerabilities rated as high or above (D).

Reference:

FortiClient EMS compliance profile configuration documentation from the study guides.

Question: 26

FortiClient EMS endpoint policies



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:

The exhibit shows multiple endpoint policies with their assigned groups, priority levels, and enabled status.

Evaluating Policy Assignment:

The Training policy is specifically assigned to the "trainingAD.training.lab" group, with a higher priority than the Default policy.

Conclusion:

The correct policy applied to the endpoint in the AD group "trainingAD" is the Training policy (A).

Reference:

FortiClient EMS policy configuration and priority management documentation from the study guides.

Question: 27

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:

The ZTNA rule configuration shown in the exhibit defines how traffic is managed and controlled based on specific tags and conditions.

Evaluating Rule Components:

The rule includes security profiles to protect traffic by applying various security checks (A).

The rule also enforces access control by determining which endpoints can access the specified resources based on the ZTNA tag (D).

Eliminating Incorrect Options:

SNAT (Source Network Address Translation) is not mentioned as part of this ZTNA rule.

The rule does not define the access proxy but uses it to enforce access control.

Conclusion:

The correct statements about the ZTNA rule are that it applies security profiles to protect traffic (A) and enforces access control (D).

Reference:

ZTNA rule configuration documentation from the study guides.

Question: 28

An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient. What must the administrator do to achieve this requirement?

A. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile

B. Disable select the vulnerability scan feature in the deployment package

C. Click the hide icon on the vulnerability scan profile assigned to endpoint

D. Use the default endpoint profile

Answer: C

Explanation:

Requirement Analysis:

The administrator needs to maintain a software vulnerability scan on endpoints without showing the feature on FortiClient.

Evaluating Options:

Disabling the feature in the deployment package or endpoint profile would remove the functionality entirely, which is not desired.

Using the default endpoint profile may not meet the specific requirement of hiding the feature.

Clicking the hide icon on the vulnerability scan profile assigned to the endpoint will keep the feature active but hidden from the user's view.

Conclusion:

The correct action is to click the hide icon on the vulnerability scan profile assigned to the endpoint (C).

Reference:

FortiClient EMS feature configuration and management documentation from the study guides.

Question: 29

Refer to the exhibit, which shows the output of the ZTNA traffic log on FortiGate.

«VMStii>n«l«33 0!1lOi«;M<91t tf'-0700»)cuprl-'0000000013" cype-nralfio' subtype'"torvaca' level'"iM>cice* va'"root"3tcip'i00.64.2.155 srcport'SeMS srcmtfpotii" arclMftol#""»an' <!«■ ip«ioc.«4,1, if dKpert"944i dir >ncf*'rooc" dor inttroIe""undeiineeP' ssccouatry»"S«aetveq" <lswcuAtEy"'»ao««d" aeaelaaid»siis ycoto-e actioa-'dany" pollcyld"0 P011cytvp«"'»roirj-poliCT" service'"wp/9W" trarrtiap'"noop" duration"# MKbpte'O ccvdbytvO omtprt'O rcvdpkt*O appcat""wiacaana-d" utMctlon*"block" countstna*! mad""Darned: failed to match a proay-pollcv" utBcef-tHtl-H

What can you conclude from the log message?

A. The remote user connection does not match the local-in policy.

B. The remote user connection does not match the ZTNA rule configuration.

C. The remote user connection does not match the ZTNA server configuration.

D. The remote user connection does not match the ZTNA firewall policy.

Answer: B

Explanation:

Observation of ZTNA Traffic Log:

The log message indicates that the remote user connection was denied due to failure to match a proxy policy.

Evaluating Log Message:

The message suggests that the connection does not match the existing ZTNA rule configuration, leading to the denial.

Conclusion:

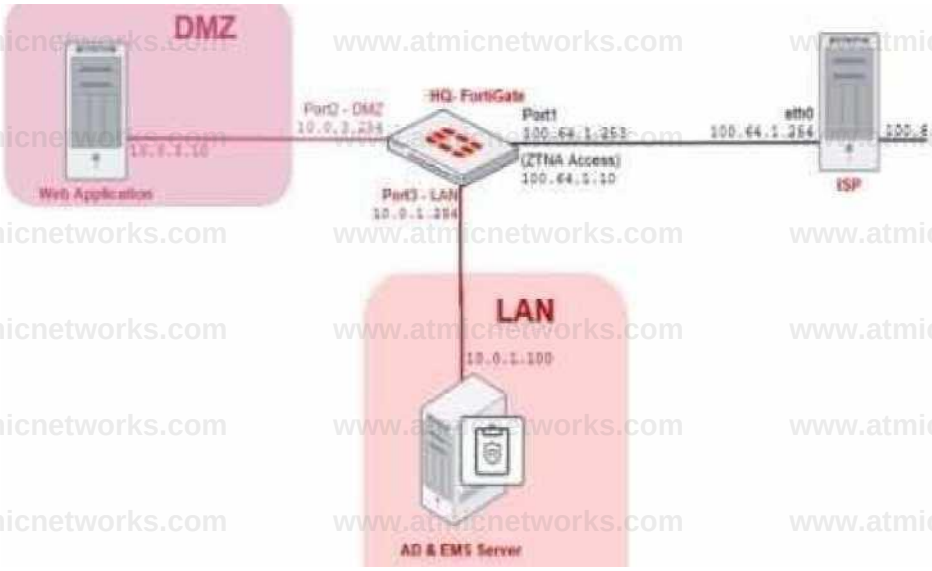
The correct conclusion from the log message is that the remote user connection does not match the ZTNA rule configuration (B).

Reference:

ZTNA traffic log analysis and configuration documentation from the study guides.

Question: 30

ZTNA Network Topology



ZTNA Rule Configuration

Name O	ZTNA A»cw
Source	■■ I
Negate Source	
ZINA Taj	Remote-men X
ZTNA Server	* ZTNA webserver
Negate Destination T>	
Action	' ACCEPT 0 DENY
Security ProWet	
AntiVirus	
Web ftier	
Video Fitter	
Application Control O	
IPS	
File Filter	O
SSL Inspection	
logging Opt Ions	
Log Allowed Trenk C	Security Events I All Sessions

Refer to the exhibits, which show a network topology diagram of ZTNA proxy access and the ZTNA rule configuration.

An administrator runs the diagnose endpoint record list CLI command on FortiGate to check RemoteClient endpoint information, however Remote-Client is not showing up in the endpoint record list.

What is the cause of this issue?

A. Remote-Client has not initiated a connection to the ZTNA access proxy.

B. Remote-Client provided an empty client certificate to connect to the ZTNA access proxy.

C. Remote-Client provided an invalid certificate to connect to the ZTNA access proxy.

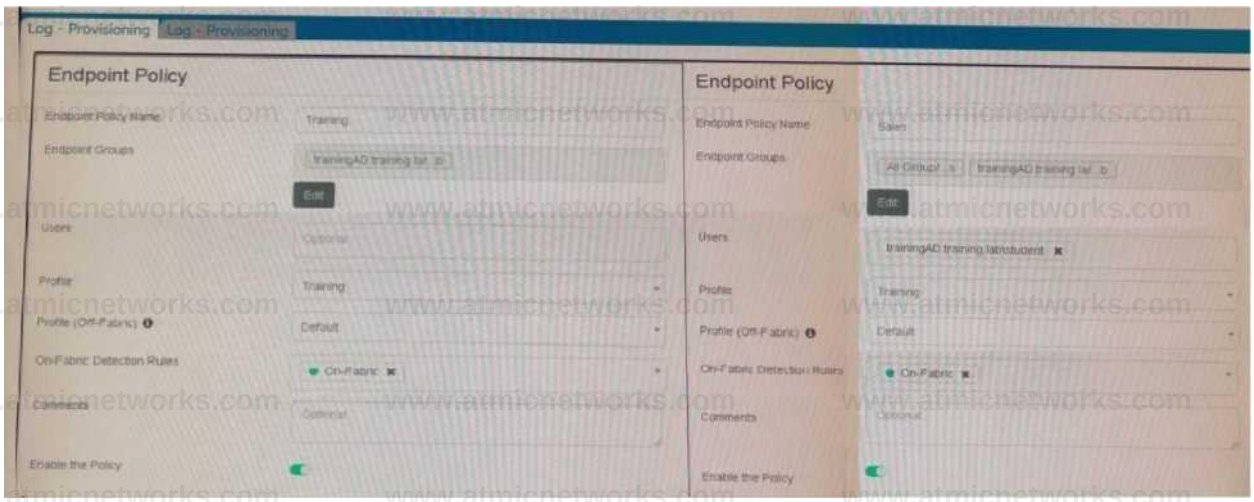
D. Remote-Client failed the client certificate authentication.

Answer: D

Explanation:

Question: 31

Refer to the exhibits.



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.

Reference

FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section

FortiClient EMS Documentation on Group Policy Assignment and Matching

Question: 32

An administrator has a requirement to add user authentication to the ZTNA access for remote or off- fabric users Which FortiGate feature is required m addition to ZTNA?

A. FortiGate FSSO

B. FortiGate certificates

C. FortiGate explicit proxy

D. FortiGate endpoint control

Answer: C

Explanation:

For adding user authentication to the ZTNA access for remote or off-fabric users, the following FortiGate feature is required in addition to ZTNA:

FortiGate explicit proxy allows FortiGate to intercept web traffic for authentication purposes.

ZTNA integrates with various FortiGate features to provide secure access and ensure that users are authenticated before accessing resources.

By using an explicit proxy, FortiGate can handle web traffic and enforce authentication policies for remote users who are not directly on the corporate network (off-fabric).

Thus, the correct feature to use for this requirement is the FortiGate explicit proxy.

Reference

FortiGate Security 7.2 Study Guide, ZTNA and Proxy Configuration Sections

Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

Question: 33

A new chrome book is connected in a school's network.

Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

A. FortiClient EMS

B. FortiClient site categories

C. FortiClient customer URL list

D. FortiClient web filter extension

Answer: D

Explanation:

For managing the FortiClient web filter extension installed on the Google Chromebook endpoint, the EMS administrator can use the following component:

FortiClient EMS (Enterprise Management Server) is designed to manage and control multiple FortiClient installations across various endpoints.

EMS provides centralized management for endpoint policies, including web filtering configurations.

The EMS administrator can configure and enforce web filter policies on Chromebooks through the EMS console.

Therefore, FortiClient EMS is the correct component for managing the web filter extension on Google Chromebook endpoints.

Reference

FortiClient EMS 7.2 Study Guide, Chromebook Management Section

Fortinet Documentation on FortiClient EMS and Web Filtering for Chromebooks

Question: 34

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

A. FortiClient EMS

B. FortiGate

C. FortiGate Access Proxy

D. 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 the same 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.

Reference :=

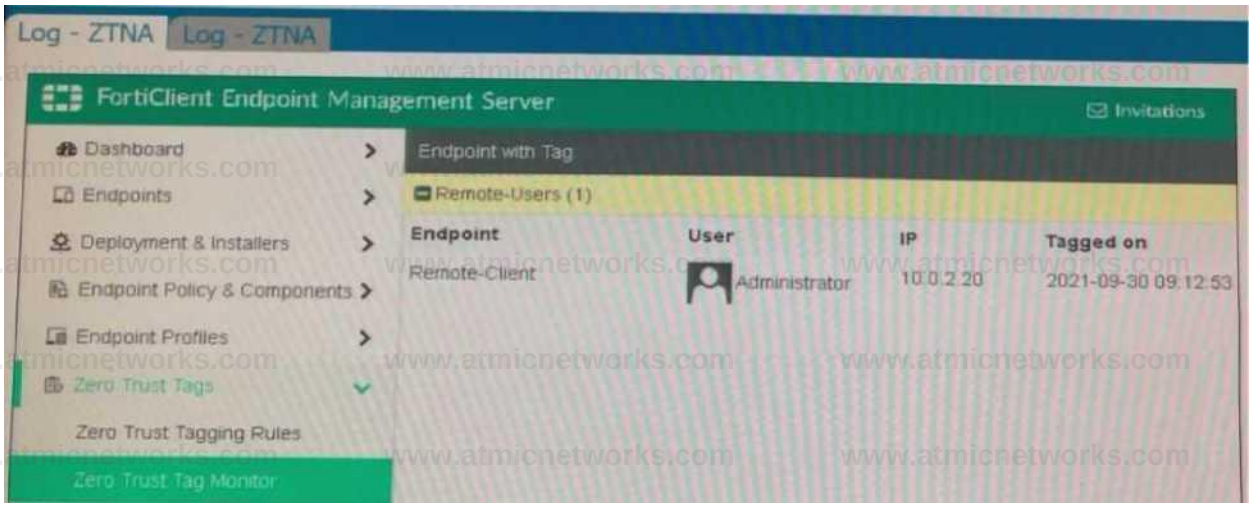
Technical Tip: Behavior of ZTNA Tags shared across multiple vdoms or multiple FortiGate firewalls in the Security Fabric connected to the same FortiClient EMS Server

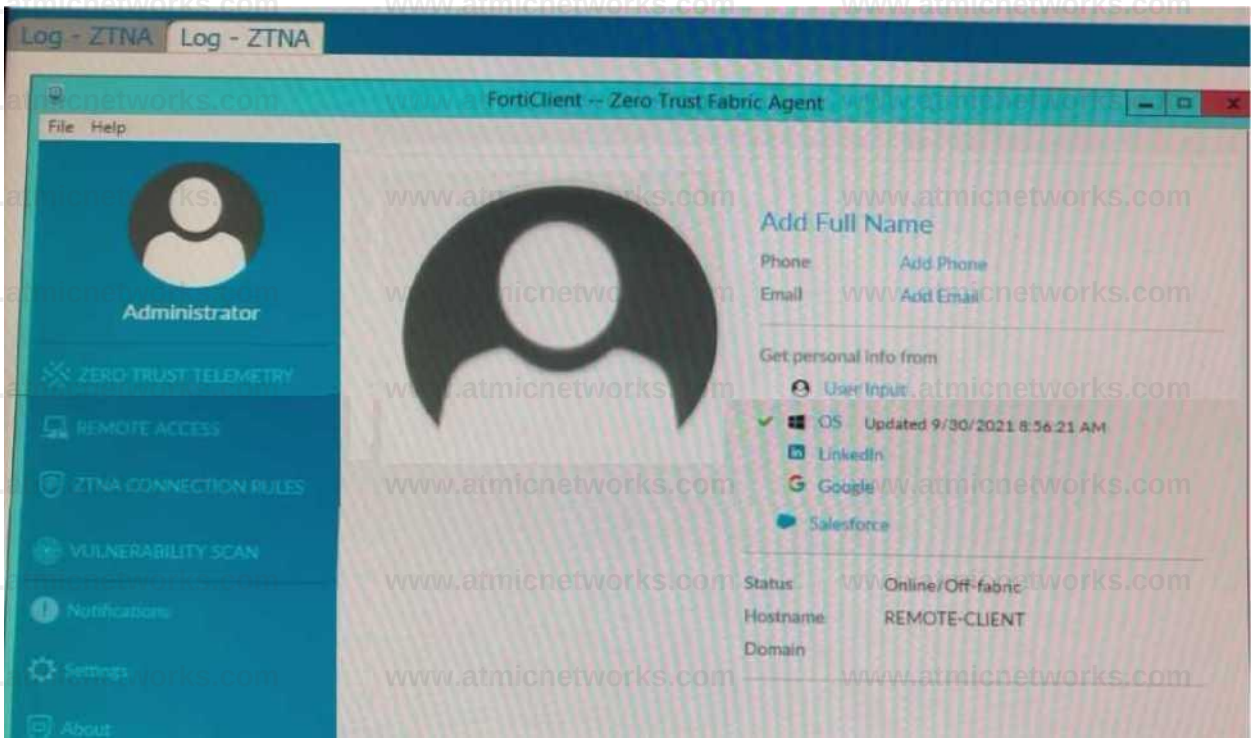
Synchronizing FortiClient ZTNA tags

Zero Trust Network Access (ZTNA) to Control Application Access

Question: 35

Refer to the exhibits.





Which show the Zero Trust Tag Monitor and the FortiClient GUI status.

Remote-Client is tagged as Remote-Users on the FortiClient EMS Zero Trust Tag Monitor.

What must an administrator do to show the tag on the FortiClient GUI?

A. Update tagging rule logic to enable tag visibility

B. Change the FortiClient system settings to enable tag visibility

C. Change the endpoint control setting to enable tag visibility

D. Change the user identity settings to enable tag visibility

Answer: B

Explanation:

Based on the exhibits provided:

The "Remote-Client" is tagged as "Remote-Users" in the FortiClient EMS Zero Trust Tag Monitor.

To ensure that the tag "Remote-Users" is visible in the FortiClient GUI, the system settings within FortiClient need to be updated to enable tag visibility.

The tag visibility feature is controlled by FortiClient system settings which manage how tags are displayed in the GUI.

Therefore, the administrator needs to change the FortiClient system settings to enable tag visibility.

Reference

FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Section

FortiClient Documentation on Tag Management and Visibility Settings

Question: 36

Which two third-party tools can an administrator use to deploy FortiClient? (Choose two.)

A. Microsoft Windows Installer

B. Microsoft SCCM

C. Microsoft Active Directory GPO

D. QR code generator

Answer: BC

Explanation:

Administrators can use several third-party tools to deploy FortiClient:

Microsoft SCCM (System Center Configuration Manager): SCCM is a robust tool used for deploying software across large numbers of Windows-based systems. It supports deployment of FortiClient through its software distribution capabilities.

Microsoft Active Directory GPO (Group Policy Object): GPOs are used to manage user and computer settings in an Active Directory environment. Administrators can deploy FortiClient to multiple machines using GPO software installation settings.

These tools provide centralized and scalable methods for deploying FortiClient across numerous endpoints in an enterprise environment.

Reference

FortiClient EMS 7.2 Study Guide, FortiClient Deployment Section

Fortinet Documentation on FortiClient Deployment using SCCM and GPO

Question: 37

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?

A. FortiAnalyzer

B. FortiClient

C. ForbClient EMS

D. Forti Gate

Answer: D

Explanation:

Question: 38

Refer to the exhibit.

```
contig user fsso edit "Server" set type fort lens set server “10.0.1.200“ set password me
ebT5)fHtMXIBykhWCSnGiFfTpi/Ej£dQu4hA424LlKxMolwn«JyX set ssI enable next
```

Based on the CLI output from FortiGate. which statement is true?

A. FortiGate is configured to pull user groups from FortiClient EMS

B. FortiGate is configured with local user group

C. FortiGate is configured to pull user groups from FortiAuthenticator

D. FortiGate is configured to pull user groups from AD Server.

Answer: A

Explanation:

Based on the CLI output from FortiGate:

The configuration shows the use of "type fortiems," indicating that FortiGate is set up to interact with FortiClient EMS.

The "server" field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.

The configuration includes an SSL-enabled connection, which is a common setup for secure communication between FortiGate and FortiClient EMS.

Thus, the configuration indicates that FortiGate is set up to pull user groups from FortiClient EMS.

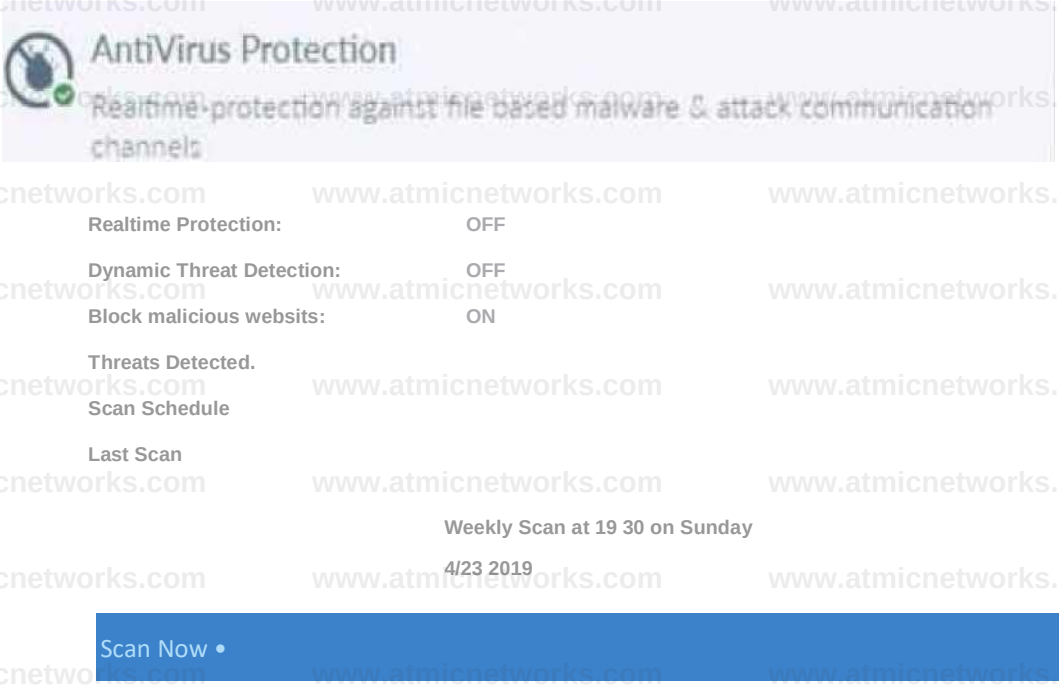
Reference

FortiGate Security 7.2 Study Guide, FSSO Configuration Section

Fortinet Documentation on FortiGate and FortiClient EMS Integration

Question: 39

Refer to the exhibit.



Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

A. Blocks the infected files as it is downloading

B. Quarantines the infected files and logs all access attempts

C. Sends the infected file to FortiGuard for analysis

D. Allows the infected file to download without scan

Answer: D

Explanation:

Block Malicious Website has nothing to do with infected files. Since Realtime Protection is OFF, it will be allowed without being scanned.

Based on the settings shown in the exhibit:

Realtime Protection: OFF

Dynamic Threat Detection: OFF

Block malicious websites: ON

Threats Detected: 75

The "Realtime Protection" setting is crucial for preventing infected files from being downloaded and executed. Since "Realtime Protection" is OFF, FortiClient will not actively scan files being downloaded. The setting "Block malicious websites" is intended to prevent access to known malicious websites but does not scan files for infections.

Therefore, when a user tries to download an infected file, FortiClient will allow the file to download without scanning it due to the Realtime Protection being OFF.

Reference

FortiClient EMS 7.2 Study Guide, Antivirus Protection Section

Fortinet Documentation on FortiClient Real-time Protection Settings

Question: 40

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 of custom 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.

Reference

FortiClient EMS 7.2 Study Guide, Deployment and Installation Section

Fortinet Documentation on FortiClient Deployment using Microsoft AD Group Policy

Question: 42

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.

Question: 43

Refer to the exhibit.

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.

Reference

FortiGate Security 7.2 Study Guide, Automation Stitches and Actions Section

Fortinet Documentation on Configuring Automation Stitches and Quarantine Actions

Question: 44

Which two VPN types can a FortiClient endpoint user inmate from the Windows command prompt? (Choose two)

A. L2TP

B. PPTP

C. IPSec

D. SSL VPN

Answer: C, D

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.

Reference

FortiClient EMS 7.2 Study Guide, VPN Configuration Section

Fortinet Documentation on Command Line Options for FortiClient VPN

Question: 45

Refer to the exhibit.

An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit.

Based on the XML settings shown in the exhibit, what must the administrator do to resolve the issue with the XML configuration file?

A. The administrator must resolve the XML syntax error.

B. The administrator must use a password to decrypt the file

C. The administrator must change the file size

D. The administrator must save the file as FortiClient-config conf.

Answer: A

Explanation:

Based on the error message and the XML configuration file shown in the exhibit:

The error "Failed to process the file" typically indicates an issue with the XML syntax.

Upon reviewing the XML content, it is crucial to ensure that all tags are correctly formatted, properly opened and closed, and that there are no syntax errors.

Resolving any XML syntax errors will allow FortiClient to successfully process and restore the configuration file.

Therefore, the administrator must resolve the XML syntax error to fix the issue.

Reference

FortiClient EMS 7.2 Study Guide, Configuration File Management Section

General XML Syntax Guidelines and Best Practices

Question: 46

Which statement about FortiClient enterprise management server is true?

A. It provides centralized management of FortiGate devices.

B. It 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.

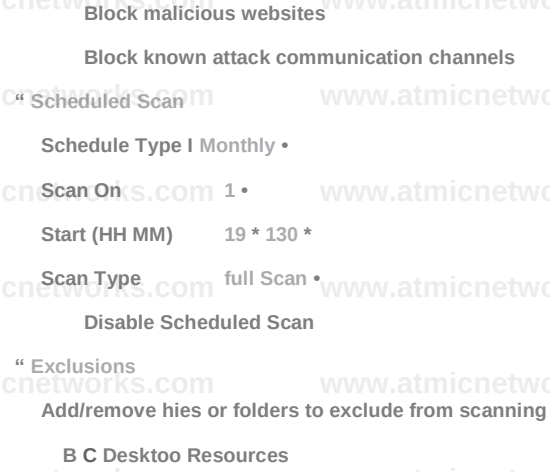
Question: 47

Refer to the exhibit.

— AntiVirus Protection •

"Settings

Son files as they are downloaded or cowed to my system Dynamic threat detection using threat intelligence data



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

Question: 48

Refer to the exhibit.

xx/xx/20xx 9:05:05 AM Notice Firewall date=20xx-xx-xx time-09:05:04 logver»2 type-traffic level=notice sessionid-34252360 hostname-Win-Internal uld-C7F302BID3EB4F05A77E38AD6202B8O7 devid-FCT8003611939390 fgtserlal-FGW010000042532 regip-N/A srcname-firefox.exe srcproduct-Firefox srcip-10.0.1.10 srcport-62401 direction-outbound destinationip-199.59.148.82 remotename-N/A destinationport=80 usen=Administrator0TRAININGAD.TRAINING.LAB proto-6 rcvdbyte»N/A sentbyte-N/A utmaction-blocked utmevent-appfirewall threat-Twitter vd-root fctver-5.4.0.0780 os-“Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy-"default“ service-http

I xx/xx/20xx 9:05:54 AM Notice Firewall date-20xx-xx-xx time-09:05:53 logver-2 type-traffic level-notice sessionid-34252360 hostname-Win-Internal uid-C7F302BID3EB4F05A77E38AD6202B8D7 devid-FCT8003611939390 fgtserial-FGVM010000042532 regip-N/A srcname-firefox.exe srcproduct-Firefox srcip-10.0.1.10 srcport-62425 direction-outbound destinationip-104.25.62.28 remotename-N/A destinationport-443 user-Administrator0TRAININGAD.TRAINING.LAB proto-6 rcvdbyte-N/A sentbyte-N/A utmaction-blocked utmevent-appfirewall threat-Proxy.Websites vd-root fctver-5.4.0.0780 os-"Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy-"default" service-https

xx/xx/20xx 9:28:23 AM Notice Firewall date-20xx-xx-xx time-09:28:22 logver-2 type-traffic level-notice sessionid-26453064 hostname-Win-Internal uld-C7F302BID3EB4F05A77E38AD6202B8D7 devid-FCT8003611939390 fgtserial-FGVM010000042532 regip-N/A srcname-firefox.exe srcproduct-Firefox srcip-10.0.1.10 srcport-62759 direction-outbound destinationip-208.71.44.31 remotename-N/A destinationport-80 user-Administrator0TRAININGAD.TRAINTNG.LAB proto-6 rcvdbyte-N/A sentbyte-N/A utmaction-blocked utmevent-appfirewall threat-Yahoo.Games vd-root fctver-5.4.0.0780 os-"Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy-"default" service-http

Based on the FortiClient logs shown in the exhibit which application is blocked by the application firewall?

A. Twitter

B. Facebook

C. Internet Explorer

D. Firefox

Answer: D

Explanation:

Based on the FortiClient logs shown in the exhibit:

The first log entry shows the application "firefox.exe" trying to access a destination IP, with the threat identified as "Twitter."

The action taken by the application firewall is "blocked" with the event type "appfirewall."

This indicates that the application firewall has blocked access to Twitter.

Reference

FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section

Fortinet Documentation on Interpreting FortiClient Logs

Question: 49

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.

Reference

FortiClient EMS 7.2 Study Guide, Real-time Protection Section

Fortinet Documentation on FortiClient Default Settings for Server Installations

Question: 50

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: B, C, E

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.

Reference

FortiClient EMS 7.2 Study Guide, Antivirus Scanning Options Section

Fortinet Documentation on Types of Antivirus Scans in FortiClient

Question: 51

Which component or device shares device status information through ZTNA telemetry?

A. FortiClient

B. FortiGate

C. FortiGate Access Proxy

D. FortiClient EMS

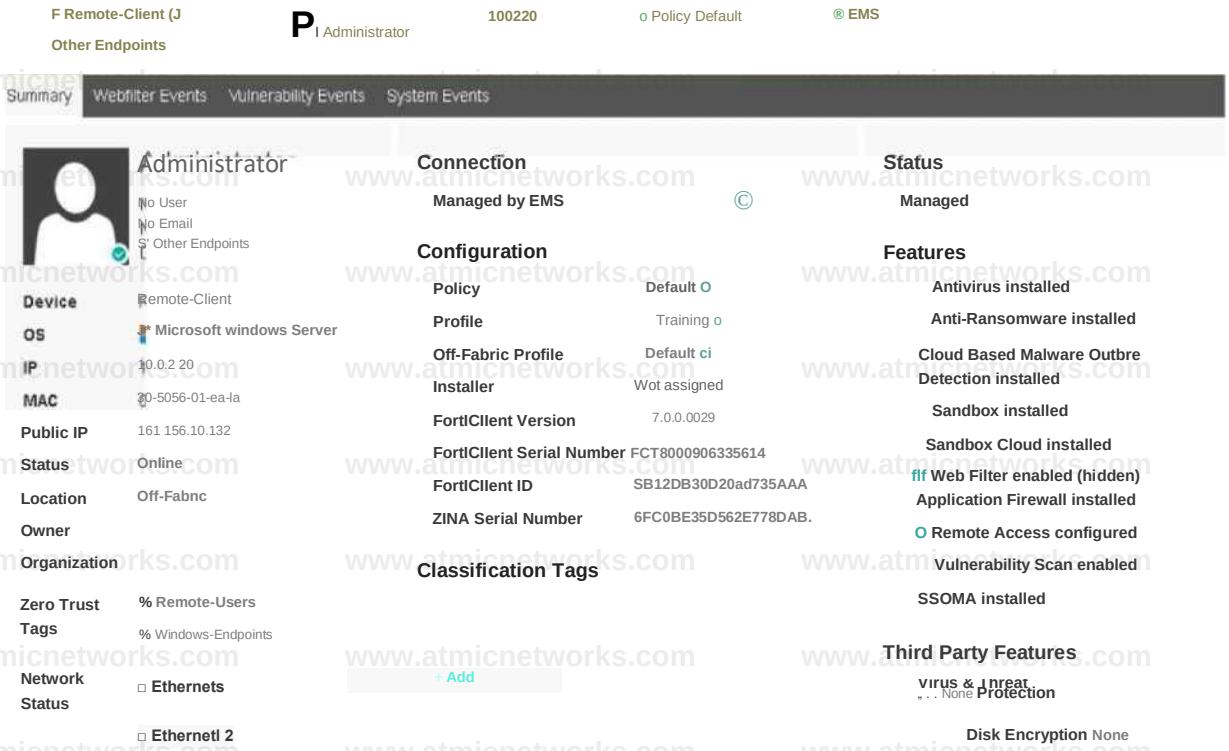
Answer: A

Explanation:

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

Question: 52

Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.



What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

A. The endpoint is classified as at risk.

B. The endpoint has been assigned the Default endpoint policy.

C. The endpoint is configured to support FortiSandbox.

D. The endpoint is currently off-net.

Answer: BD

Explanation:

Based on the Remote-Client status shown in the exhibit:

Endpoint Policy: The "Policy" field shows "Default," indicating that the endpoint has been assigned the Default endpoint policy.

Connection Status: The "Location" field shows "Off-Fabric," meaning that the endpoint is currently off the corporate network (off-net).

Therefore, the two conclusions that can be made are:

The endpoint has been assigned the Default endpoint policy.

The endpoint is currently off-net.

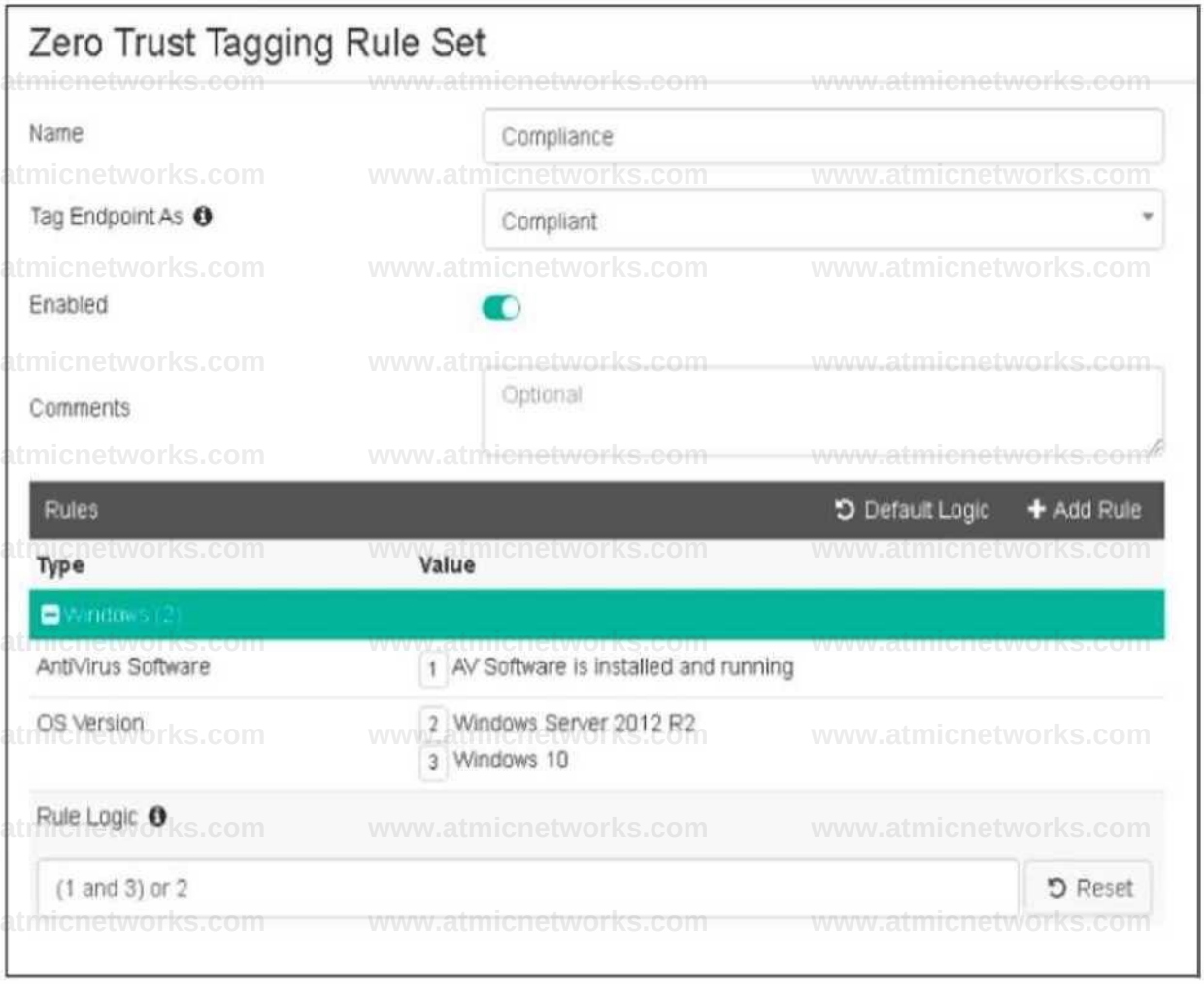
Reference

FortiClient EMS 7.2 Study Guide, Endpoint Summary Information Section

Fortinet Documentation on Endpoint Policies and Status Indicators

Question: 53

Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.



Which two statements about the rule set are true? (Choose two.)

A. The endpoint must satisfy that only Windows 10 is running.

B. The endpoint must satisfy that only AV software is installed and running.

C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.

D. The endpoint must satisfy that only Windows Server 2012 R2 is running.

Answer: CD

Explanation:

Based on the Zero Trust Tagging Rule Set configuration shown in the exhibit:

The rule set includes two conditions:

AV Software is installed and running

OS Version is Windows Server 2012 R2 or Windows 10

The Rule Logic is specified as "(1 and 3) or 2," meaning:

The endpoint must have antivirus software installed and running and must be running Windows 10.

Alternatively, the endpoint must be running Windows Server 2012 R2.

Therefore, the endpoint must satisfy either:

Antivirus is installed and running and Windows 10 is running.

Windows Server 2012 R2 is running.

Reference

FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Rule Set Configuration Section

Fortinet Documentation on Configuring Zero Trust Tagging Rules and Logic

Question: 54

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: C, D

Explanation:

Question: 55

Which statement about the FortiClient enterprise management server is true?

A. It receives the configuration information of endpoints from ForuGate.

B. It provides centralized management of multiple endpoints running FortiClient software.

C. It enforces compliance on the endpoints using tags

D. It receives the CA certificate from FortiGate to validate client certrficates.

Answer: C

Explanation:

Question: 56

An administrator must deploy FortiClient for an organization that has BYOD and remote users.

What can the administrator use to deploy FortiClient? (Choose one answer)

A. FortiClient zero-touch provisioning

B. Microsoft System Center Configuration Manager (SCCM)

C. Microsoft Intune

D. Group Policy Object (GPO)

Answer: C

Explanation:

According to the FortiClient EMS Administrator Study Guide and the Fortinet Document Library (7.2/7.4 versions), the most effective method for deploying FortiClient to BYOD (Bring Your Own Device) and remote users is using Microsoft Intune (or other supported Mobile Device Management - MDM solutions).

1. Why Microsoft Intune (Answer C) is the Correct Choice:

Cloud-Based Accessibility: Unlike GPO or SCCM, which traditionally require a direct connection to the local Active Directory (AD) domain or a VPN to reach the on-premises infrastructure, Microsoft

Intune is a cloud-based MDM. This makes it the native choice for remote users who may not always be on the corporate network.

BYOD Management: Intune is specifically designed to manage a variety of operating systems (Windows, macOS, iOS, Android) that are common in BYOD environments. It allows administrators to push the FortiClient installation

package and enrollment configuration (such as the invitation_code or ems_server details) directly to the user's device via the cloud.

Integration with EMS: FortiClient EMS 7.2/7.4 provides specific documentation for Intune Integration. Administrators can create a custom MSI or .pkg installer in EMS, upload it to Intune, and use Intune's app configuration policies to automate the Telemetry connection to EMS.

2. Why Other Options are Incorrect for this Scenario:

A . FortiClient zero-touch provisioning: While FortiClient supports zero-touch provisioning (particularly for mobile or through FortiCloud), in the context of a "deployment tool" for an organization's broad BYOD and remote fleet, it is typically a feature or process facilitated by an MDM like Intune rather than the standalone deployment mechanism for the initial software package on third-party remote devices.

B . Microsoft SCCM: SCCM (now part of Microsoft Configuration Manager) is heavily reliant on onpremises infrastructure and is generally used for corporate-owned, domain-joined devices. It is less flexible than Intune for managing "unmanaged" BYOD devices belonging to remote users.

D . Group Policy Object (GPO): GPO requires the device to be joined to the Active Directory (AD) Domain. BYOD devices are typically not domain-joined, and remote devices cannot receive GPO updates unless they are connected via VPN at the time of the policy refresh, making it unsuitable for this specific use case.

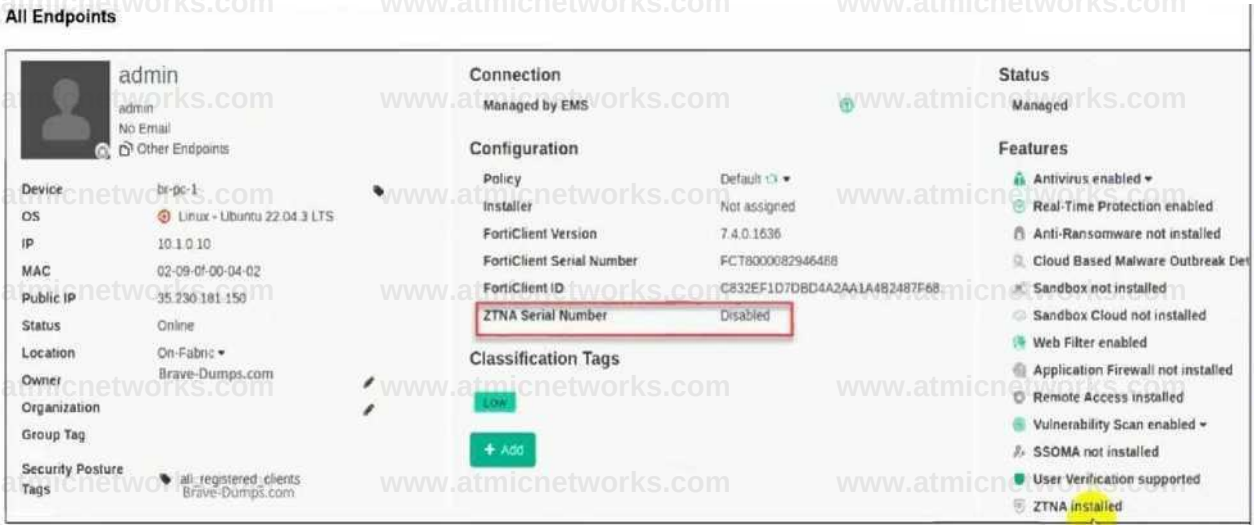
3. Curriculum Reference:

EMS Administration Guide (Deployment Section): Specifies that for endpoints not reachable via AD/Workgroups (which covers remote and BYOD), administrators should use the Installer Link method or an MDM (like Microsoft Intune).

Intune Deployment Guide for FortiClient: Detail the specific use of Configuration Keys (e.g., cloud_invite_code, ems_server) that are passed from Intune to the FortiClient app to ensure that once the remote user installs the app, it automatically registers to the correct EMS instance.

Question: 57

Refer to the exhibit.



The zero trust network access (ZTNA) serial number on endpoint br-pc-1 is in a disabled state.

What is causing the problem? (Choose one answer)

A. The ZTNA feature is not installed on FortiClient.

B. The ZTNA destinations endpoint profile is disabled.

C. The ZTNA is disabled due to FortiClient disconnected from FortiClient EMS.

D. The ZTNA certificate has been revoked by administrator.

Answer: B

Explanation:

Based on the FortiClient EMS 7.2/7.4 Study Guides and the visual evidence provided in the exhibit, here is the verified breakdown of why the ZTNA Serial Number is showing as Disabled:

1. Analysis of the Exhibit

Operating System: The endpoint is running Linux (Ubuntu 22.04.3 LTS).

Connection Status: The endpoint status is Online and Managed by EMS. This immediately eliminates Option C, as the device is actively communicating with the EMS server.

Features List: At the bottom right of the "Features" column, it explicitly states "ZTNA installed". This eliminates Option A, confirming the software component is present on the endpoint.

ZTNA Serial Number Field: The field is highlighted in red and shows "Disabled".

2. Identifying the Root Cause (Option B)

In the FortiClient EMS curriculum regarding ZTNA (Zero Trust Network Access), the ZTNA Serial Number (also known as the ZTNA Tagging or Client Certificate UID) is generated and activated based on the assigned Endpoint Profile.

Profile Dependency: For FortiClient to generate a ZTNA serial number/certificate and participate in ZTNA, the administrator must enable and configure the ZTNA Destinations (or ZTNA Connection) profile within the EMS.

Disabled State: If the ZTNA Destinations feature is disabled in the profile assigned to that specific endpoint (or if the endpoint is assigned the "Default" profile where ZTNA is not configured), the "ZTNA Serial Number" status on the EMS dashboard will reflect as Disabled.

Linux Specifics: In FortiClient for Linux, ZTNA support is available but requires the profile to be explicitly pushed and active. If the profile is toggled off in the EMS GUI under Endpoint Profiles > ZTNA Destinations, the serial number functionality is suspended.

3. Why Other Options are Incorrect

A . The ZTNA feature is not installed: The exhibit clearly shows "ZTNA installed" under the Features list.

C . FortiClient disconnected from EMS: The exhibit shows the status as "Online" and "Managed by EMS" with a green checkmark.

D . The ZTNA certificate has been revoked: If a certificate is revoked, the status typically shows as "Revoked" or "Expired," or the serial number would still be present but marked as untrusted. A "Disabled" state indicates the feature itself is turned off at the policy/profile level.

Question: 58

Refer to the exhibit.

FortiCIlent logs

```
28250226 05:50:24.563 TZ-+0100 [DEBUG] proxy:3bl ConnlD 1557243034: now rate bte.COM 7
20250226 05:50:24.563 TZ*f0100 [DEBUG] accessors:127 url comparing https://www.twltter.cOM https://bbc.coia
20250226 05:50:24.563 TZ-+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /
20250226 05:50:24.564 TZ-+0100 [ERROR] ratlng_db:97 Category query failure; failed to UrlRequestSendReceive
receiveResponse error: FortlGuard server down, task dropped, https bbc.COM / Brave-Durnps.com /
20250226 05:50:24.564 TZ-+0100 [INFO ] proxy:383 ConnlD 1557243034: bbc.com / rating: -1 action: WF_4CTI0HJL0CK
20250226 05:50:24.564 TZ-+0100 (INFO ] accessors:352 Inserting violation: (bbc.com / Unknown 2025-02-26 05:50:24.564598172
+0100 CET m-+4561.038040408 admin 368039 /opt/google/chrome/chrome)
20250226 05:50:24.601 TZ-+0100 [DEBUG] http2_handler;312 set table size to 65536
20250226 05:50:24.820 TZ-+0100 [DEBUG] proxy:381 ConnlD 1557243034: now rate bbc.com /favicon.ico
20250226 05:50:24,820 TZ-+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com/favicon.ico
20250226 05:50:24.820 TZ++0100 [DEBUG] fgdahandle:346 Category request: host bbc.com oath /favicon.lco
20250226 05:50:24.821 TZ-+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortlGuard server down, task dropped, https bbc.com /favicon.ico Brave Dumps.com
20250226 05:50:24.821 T2-+0100 [INFO ] proxy:383 ConnlD 1557243034: bbc.com /favicon.ico rating: -1 action: WF_ACTION SLOCK
20250226 05:50:24.821 TZ-S0100 [INFO ] accessors:352 Inserting violation: (bte.coM /favicon.ico Unknown 2025-02 26 05:50:24.8212255: +0100 CET m=+4561.294667764 admin
368039 /cpt/google/chrome
```

Why is the user not able to access bbc.com? (Choose one answer)

A. The URL is blocked by the web filter endpoint profile.

B. The endpoint cannot resolve the URL FQDN.

C. FortiGuard servers are not reachable from the endpoint.

D. The application firewall is blocking Google Chrome.

Answer: C

Explanation:

Based on the FortiClient EMS Administrator Study Guide regarding Web Filter troubleshooting and the specific log entries provided in the exhibit, the reason the user cannot access the website is due to connectivity issues with FortiGuard.

1. Analysis of the FortiClient Logs:

The Error Message: The logs show multiple [ERROR] entries stating: rating_db:97 Category query failure: failed to UrlRequestSendReceive.

Root Cause Identity: The log explicitly describes the failure: receiveResponse error: FortiGuard server down, task dropped, https bbc.com.

Resulting Action: Because the endpoint could not receive a rating from the FortiGuard servers, the Web Filter module recorded rating: -1 and applied the action WF_ACTION_BLOCK.

2. Why Option C is Correct:

FortiGuard Dependency: FortiClient's Web Filter module relies on real-time queries to FortiGuard distribution servers to categorize URLs. If the endpoint is behind a firewall blocking FortiGuard ports (typically UDP 53 or 8888, or HTTPS 443) or has no internet path to these servers, it cannot categorize the site.

Fail-Safe Behavior: In many FortiClient configurations, if a rating cannot be obtained (Category query failure), the default security posture is to block the request to ensure no potentially malicious or unrated "Unknown" sites are accessed. The logs confirm this by showing the "FortiGuard server down" message immediately followed by the block action.

3. Why Other Options are Incorrect:

A . The URL is blocked by the web filter endpoint profile: If it were a standard profile block, the log would show a specific Category ID (e.g., Category 52 for News and Media) being blocked by policy. Instead, it shows a rating failure (-1).

B . The endpoint cannot resolve the URL FQDN: The logs show the process correctly identifies host bbc.com. If DNS

had failed, the proxy wouldn't even reach the stage of attempting a FortiGuard category query for that specific URL.

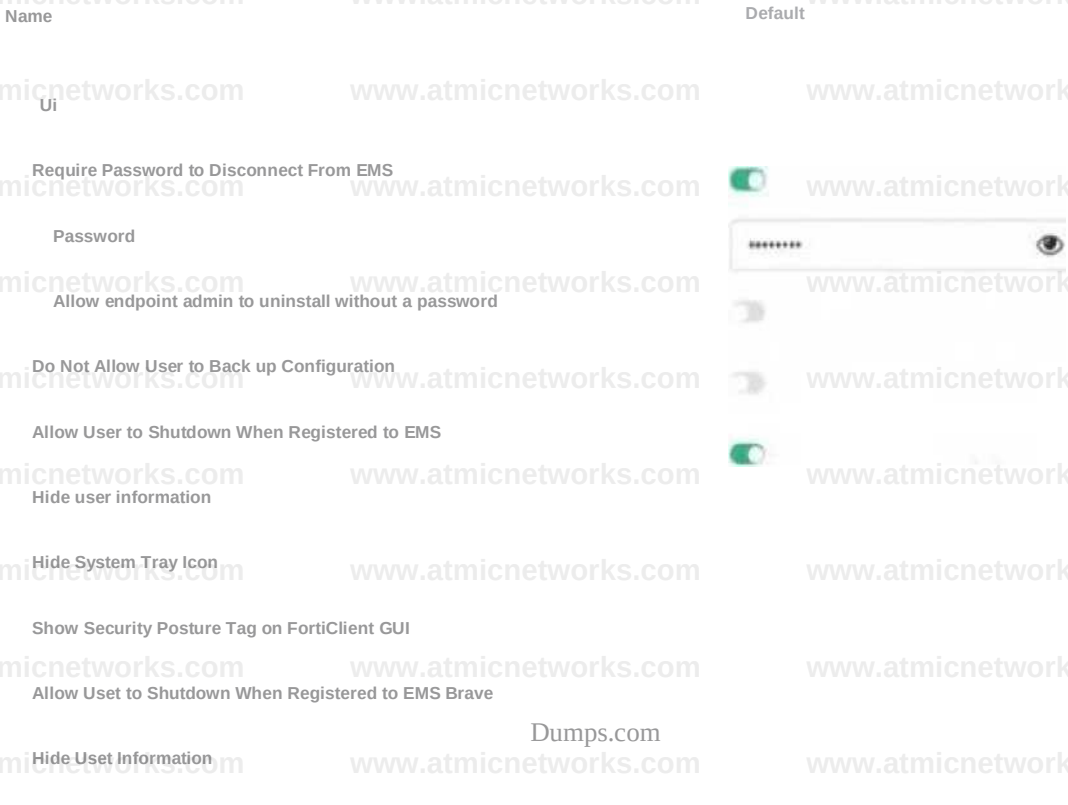
D . The application firewall is blocking Google Chrome: While the log mentions /opt/google/chrome/chrome, the error is generated by the rating_db and proxy components of the Web Filter, not the Application Firewall module.

Question: 59

Refer to the exhibit.

System settings profile

System Settings Profile



Which behavior should you expect when FortiClient with an invalid certificate is connecting to FortiClient EMS? (Choose one answer)

A. FortiClient is blocked from connecting to FortiClient EMS.

B. FortiClient requires an additional password to connect to FortiClient EMS.

C. FortiClient displays a warning message to the end user.

D. FortiClient EMS pushes a valid certificate to FortiClient.

Answer: C

Explanation:

Based on the FortiClient EMS 7.2/7.4 Administration Guide and the provided exhibit of the System Settings Profile, the expected behavior for an invalid certificate connection is determined by the Invalid Certificate Action setting.

1. Analysis of the Exhibit

Location: The exhibit shows the System Settings Profile (specifically the "Default" profile).

Setting: At the bottom under the Endpoint Control section, the field Invalid Certificate Action is configured.

Selected Action: The dropdown for Invalid Certificate Action displays a warning icon (an orange triangle with an exclamation mark). In the FortiClient EMS GUI, this specific icon corresponds to the "Warn" action.

2. Verified Behavior (Option C)

According to the curriculum documents regarding Endpoint Communication Security:

Warn Action Behavior: When the Invalid Certificate Action is set to Warn, FortiClient is instructed to display a warning message to the end user if the EMS server certificate is untrusted, expired, or has a hostname mismatch.

User Prompt: The warning message explicitly asks the user whether they wish to proceed with the connection despite the security risk or terminate the attempt.

Connection Logic: If the user manually accepts the warning, FortiClient will establish the Telemetry connection and "remember" the certificate for future sessions to avoid repeated prompts for that specific server.

3. Why Other Options are Incorrect

A . FortiClient is blocked: This behavior only occurs if the administrator selects the "Deny" action in the profile.

B . Additional password required: The password field shown at the top of the exhibit is for "Require

Password to Disconnect From EMS", which prevents users from manually unregistering, but it does not bypass or resolve certificate errors.

D . EMS pushes a valid certificate: EMS cannot "push" a valid identity certificate to resolve a failed TLS handshake; a valid certificate must be manually installed on the EMS server by the administrator.

Question: 60

An administrator has lost web access to the FortiClient EMS console, and the web page to access to the console is timing out.

How can the administrator gather information to investigate the issue? (Choose one answer)

A. Use the CLI diagnostic tool on the EMS server.

B. Download the webserver logs from the PostgreSQL server.

C. Use the diagnostic logs option from the FortiClient EMS GUI.

D. Download the log generator from the support site and run it on the EMS server.

Answer: A

Explanation:

According to the FortiClient EMS Administrator Study Guide and official Technical Tips from Fortinet, when the web console is inaccessible (e.g., timing out), the administrator must use tools available directly on the server's operating system (CLI) to gather diagnostic information.

1. Why the CLI Diagnostic Tool (Answer A) is the Correct Choice:

Availability during Outage: When the GUI is unreachable, the standard "Generate Diagnostic Logs" option within the EMS interface is also unavailable.

Windows-based EMS: The administrator can manually run the EMSDiagnosticTool.exe located at C:\Program Files (x86)\Fortinet\FortiClientEMS\. This tool collects server information, Windows events, and EMS-specific logs into a compressed file for investigation.

Linux-based EMS (v7.4+): For newer versions running on Linux, the administrator can use the CLI command: sudo /opt/forticlientems/bin/diagnostic_tool -o /tmp/diag to generate a diagnostic package.

Service Verification: The CLI also allows administrators to verify if critical services (like fcems, apache2, or postgres) are running or if remote access has been disabled using the emscli utility.

2. Why Other Options are Incorrect:

B . Download webserver logs from PostgreSQL: PostgreSQL is the database engine for EMS, not the web server. While

database logs are useful, they are not the primary method for gathering general "diagnostic information" and would typically be collected as part of the CLI diagnostic tool output rather than downloaded directly from the DB.

C . Diagnostic logs option from the GUI: This option is impossible to use if the administrator has lost web access and the page is timing out.

D . Download log generator from support site: While Fortinet provides various tools on their support site, the EMS Diagnostic Tool is natively installed with the FortiClient EMS software and is the primary, documented method for troubleshooting the EMS server itself.

Question: 61

When multitenancy is enabled on FortiClient EMS, which administrator role can provide access to the global site only? (Choose one answer)

A. Tenant administrator

B. Settings administrator

C. Standard administrator

D. Global administrator

Answer: B

Explanation:

According to the FortiClient EMS Administration Guide (specifically the sections on Multitenancy), when multitenancy is enabled, the system introduces specific administrator roles to manage the separation between global settings and individual sites.

1. The Settings Administrator Role (Answer B)

Specific Scope: The Settings administrator is a specialized role designed to have access to the global site only.

Permissions: This role can access all configuration options on the global site, with the notable exception of administrator configuration (they cannot create or manage other admin accounts).

Use Case: This is typically used for auditors or system managers who need to oversee global-level configurations without needing access to specific endpoint data within individual sites or the power to modify administrative users.

2. Comparison with Other Multitenancy Roles

Super administrator: This role has unlimited access to the global site and all other sites within the EMS instance.

Site administrator: This role is restricted to specified sites only and has no access to the global site.

Standard administrator (Answer C): This is a generic role level within a site or a single-tenant environment but is not the role that defines "global-only" access in a multitenant setup.

Tenant administrator / Global administrator: While these terms are common in general IT, FortiClient EMS documentation specifically uses the titles Super, Settings, and Site administrators for multitenancy management.

3. Curriculum Reference

FortiClient EMS 7.2/7.4 Study Guide (Multitenancy Chapter): Explicitly lists "Settings administrator" as the role providing access to the global site only.

Admin Roles Table: The documentation provides a comparison table where the Settings Administrator's scope is strictly defined as "Global site only".

Question: 62

Which Fortinet solution can you integrate FortiClient with to use the single sign-on mobility agent (SSOMA) feature? (Choose one answer)

A. FortiAuthenticator

B. FortiSASE

C. FortiPAM

D. FortiNAC

Answer: A

Explanation:

According to the FortiClient EMS 7.2/7.4 Administration Guide and FortiAuthenticator Study Guides, the Single Sign-On Mobility Agent (SSOMA) is a feature specifically designed to integrate with FortiAuthenticator to provide transparent, identity-based authentication.

1. Integration with FortiAuthenticator (Answer A)

The SSOMA Service: The mobility agent service is hosted on the FortiAuthenticator unit. Administrators must navigate to Fortinet SSO Methods > SSO > General on the FortiAuthenticator and toggle on Enable FortiClient SSO Mobility Agent Service.

Communication Protocol: FortiClient communicates with FortiAuthenticator via a specified TCP listening port (defaulting to 8001 or 8005) and uses a pre-shared key (secret key) for authentication.

Transparent Authentication: Once configured, the SSOMA on the endpoint automatically sends user logon information and

IP address changes (such as WiFi roaming) to FortiAuthenticator.

FortiAuthenticator then shares this information with FortiGate units to enforce identity-based security policies without the user needing to re-authenticate manually.

2. Modern Capabilities (Azure AD / Entra ID)

Cloud Integration: In FortiClient 7.2.1 and later, SSOMA supports native Azure AD (Entra ID). In this mode, the agent sends the Azure AD domain and tenant ID directly to FortiAuthenticator, allowing organizations to create identity-based policies for cloud-joined devices.

3. Note on FortiPAM (Option C)

Recent Updates: While recent FortiClient EMS 7.4 documentation mentions an "Add FortiPAM agent to SSOMA" feature, this is an extension of the existing SSOMA framework. The core product that defines and runs the SSOMA service for general Single Sign-On (SSO) remains FortiAuthenticator.

4. Why Other Options are Incorrect

B . FortiSASE: While FortiSASE uses FortiClient for Secure Internet Access (SIA), it uses different mechanisms (like SAML or the SASE cloud portal) for user identity rather than the specific SSOMA agent service.

D . FortiNAC: FortiNAC uses FortiClient for persistent agent-based posture assessment and scanning, but it does not utilize the SSOMA mobility agent for user-to-IP mapping.

Question: 63

Which two statements about FortiClient EMS integration with Active Directory (AD) are true?

(Choose two answers)

A. FortiClient EMS has full read-write access on the AD server.

B. FortiClient installations on domain endpoints can deployed from FortiClient EMS.

C. Endpoint profiles can be assigned to endpoints based on domain groups.

D. Imported AD endpoints cannot be directly deleted on FortiClient EMS

Answer: BC

Explanation:

Based on the FortiClient EMS 7.2/7.4 Administration Guide and the EMS Administrator Study Guide, the integration with Active Directory (AD) provides several automated management capabilities.

1. Analysis of the True Statements:

B . FortiClient installations on domain endpoints can be deployed from FortiClient EMS:

FortiClient EMS allows administrators to create Deployment Profiles specifically for Windows endpoints discovered via AD.

By providing AD administrator credentials within the deployment profile, EMS can remotely push the FortiClient MSI installer to domain-joined endpoints that do not yet have the software installed.

C . Endpoint profiles can be assigned to endpoints based on domain groups:

The core benefit of AD integration is the ability to map Endpoint Policies to specific AD Organizational Units (OUs) or Security Groups.

When an endpoint policy is assigned to an AD group, all FortiClient endpoints belonging to that group automatically receive the associated security profiles (Antivirus, Web Filter, VPN, etc.) defined within that policy.

2. Why Other Options are Incorrect/Secondary:

A . FortiClient EMS has full read-write access on the AD server:

The curriculum states explicitly that the LDAP/AD connection is read-only.

EMS cannot modify AD objects, create users, or change group memberships; it only synchronized information from the AD server to the EMS database.

D . Imported AD endpoints cannot be directly deleted on FortiClient EMS:

While technically true in a functional sense (deleting a synced endpoint will result in it being readded during the next sync unless it is removed from the AD OU), the curriculum typically prioritizes B and C as the primary functional "features" of the integration.

Note that the guide specifies the "Delete" action in the Endpoints pane is restricted to non-domain devices to prevent synchronization conflicts.

3. Summary of Integration Features:

Sync Schedule: EMS periodically syncs with AD (default every 10 minutes) to update the endpoint list.

Policy Automation: Moving a user or computer to a different group in AD will cause EMS to automatically update their security posture based on the new group's assigned policy.

Question: 64

Which two statements apply to FortiClient forensics analysis? (Choose two answers)

A. FortiClient sends an alert notification when malicious activity is triggered.

B. The administrator must request analysis for the desired endpoint.

C. The endpoint is quarantined until forensics is completed.

D. Forensics analysis features must be enabled in the system settings profile.

Answer: BD

Explanation:

Based on the FortiClient EMS 7.2/7.4 Administrator Study Guide and the FortiGuard Forensics Service User Guide, the forensics analysis feature is a specialized service that requires specific administrative actions and configuration.

1. The Administrator Must Request Analysis (Answer B)

Manual Initiation: Unlike standard Antivirus or Sandbox scans which occur automatically upon detection, the FortiGuard Forensics Analysis is a service-based investigation.

Workflow: Once a threat is detected or a device is suspected of being compromised, the administrator must navigate to the Endpoints pane, select the specific device, and click the Request Analysis button.

Escalation: The administrator then fills out a questionnaire (providing the reason for escalation and issue summary) to submit the logs to the FortiGuard Labs forensic team for manual review.

2. Forensics Features Must be Enabled in the Profile (Answer D)

Two-Step Enabling:

Global Level: First, the feature must be toggled on under System Settings > Feature Select > FortiGuard Forensics Analysis.

Profile Level: Crucially, it must be enabled within the Endpoint Profile (specifically under System Settings) that is applied to the target endpoints.

Agent Deployment: Toggling this in the profile ensures the FortiClient endpoint prepares the "forensics agent" components required to collect deep-system data (such as the Master File Table, Windows Event Logs, and registry hives) when a request is eventually made.

3. Why Other Options are Incorrect

A . FortiClient sends an alert notification: While FortiClient does send alerts for malicious activity, this is part of the standard Endpoint Control and Malware Protection modules. The forensics analysis itself is the follow-up investigation performed after such an alert is received and reviewed by an admin.

C . The endpoint is quarantined until completed: Although it is a security "Best Practice" to quarantine a compromised endpoint during an investigation, the forensics analysis process does not programmatically force or require a quarantine state to function. The forensics agent can collect logs from an online, non-quarantined device as long as it has

EMS connectivity.

Question: 65

Refer to the exhibit.

You provide a webserver hosting service. An endpoint downloads a test file, testfile.txt, that gets blocked by FortiClient.

Which configuration can you use to make the file accessible on the endpoint? (Choose one answer)

A. Restore access to file directly using FortiClient.

B. Allow the webserver URL in the exclusion list in the web filter profile.

C. Exclude testfile.txt from the malware protection profile.

D. Add the file to the allowlist in quarantine management on FortiClient EMS.

Answer: D

Explanation:

According to the FortiClient EMS 7.2/7.4 Administration Guide (specifically the Quarantine Management and Malware Protection sections), the correct administrative workflow to restore a blocked file and ensure it is no longer flagged as malicious is to use the Quarantine Management feature on the EMS server.

1. Analysis of the Exhibit

Event Type: The exhibit shows an Antivirus Event where a file named testfile.txt was flagged as Malware: EICAR_TEST_FILE.

Location: The file was found in a local user directory (C:\Users\administrator\Desktop\Resources\testfile.txt).

System State: The endpoint is managed by EMS (indicated by the Policy: Default and EMS status icons).

2. Why Option D is the Correct Choice:

Centralized Control: In a managed environment, the administrator uses the EMS console to oversee security incidents. To restore a file that has been quarantined, the administrator must navigate to Quarantine Management > Files.

Allowlist & Restore Action: By selecting the specific blocked file (testfile.txt) and clicking Allowlist & Restore, two things happen simultaneously:

Restoration: EMS sends a command to the FortiClient endpoint to release the file from the local quarantine folder and return it to its original path.

Allowlisting: The file's hash is added to the Allowlist (managed under Quarantine Management > Allowlist), which prevents FortiClient from re-quarantining the file during future real-time or on-demand scans.

Accessibility: This is the documented method to make a file "accessible on the endpoint" while ensuring it is not immediately re-blocked by the security engine.

3. Why Other Options are Incorrect:

A . Restore access directly using FortiClient: While FortiClient has a local quarantine tab, the "Release" button is typically greyed out or restricted when the client is managed by EMS to ensure centralized security policy enforcement.

B . Allow the webserver URL in the exclusion list: The exhibit shows an Antivirus/Malware event, not a Web Filter event. The file has already been downloaded to the local disk and is being blocked by the Real-Time Protection engine, so a Web Filter URL exclusion would have no effect on the local file block.

C . Exclude testfile.txt from the malware protection profile: While adding a path exclusion to the Malware Protection profile is a valid way to prevent future scans of a directory, it does not automatically restore a file that has already been moved to quarantine. The proper workflow for an existing block is to use the Quarantine Management tool first.

Question: 66

A company must integrate the FortiClient EMS with their existing identity management infrastructure for user authentication, and implement and enforce administrative access with multifactor authentication (MFA). Which two authentication methods can they use in this scenario? (Choose two answers)

A. LDAPS

B. RADIUS

C. TACACS

D. SAML

Answer: BD

Explanation:

According to the FortiClient EMS 7.4 Administration Guide, for an organization to integrate with an identity management infrastructure while enforcing administrative access with Multi-Factor Authentication (MFA), the primary supported methods for remote administrator authentication are

RADIUS and SAML.

1. RADIUS (Answer B)

Identity Integration: FortiClient EMS allows administrators to add RADIUS servers as an authentication source under the Administration > Authentication Servers section.

MFA Support: RADIUS is a standard protocol for enforcing MFA. In this scenario, FortiClient EMS acts as a RADIUS client to an external MFA provider (such as FortiAuthenticator, RSA Authentication Manager, or Duo).

Workflow: When an administrator attempts to log in to the EMS console, EMS sends an AccessRequest to the RADIUS server. If the provider requires MFA, it can challenge the user (via push notification or token code) before sending an Access-Accept back to EMS.

2. SAML (Answer D)

Modern Identity Management: SAML (Security Assertion Markup Language) is the preferred method for integrating with modern cloud and on-premises Identity Providers (IdPs) like Microsoft Entra ID (formerly Azure AD), Okta, AD FS, or FortiAuthenticator.

Native MFA Enforcement: By using SAML SSO, the authentication and MFA process are handled entirely by the IdP. The EMS server acts as the Service Provider (SP). When an admin logs in, they are redirected to the IdP, where the company's existing MFA policies (Conditional Access, etc.) are enforced before the user is granted access back to the EMS console.

EMS Configuration: The curriculum details specific SAML SSO configurations for various IdPs under the SAML SSO section of the Administration Guide.

3. Why Other Options are Incorrect/Insufficient

A . LDAPS: While FortiClient EMS supports importing users from Active Directory (ADDS) via LDAP/LDAPS for endpoint management and basic admin login, standard LDAPS does not natively support or enforce an MFA challenge-response workflow in the same integrated way that RADIUS or SAML does for administrative console access.

C . TACACS: TACACS+ is primarily used for device administration on networking equipment (like FortiGate) and is not a listed or standard method for administrative authentication within the FortiClient EMS software documentation.

Question: 67

A FortiClient EMS administrator is implementing additional security on FortiClient for compliance checks. Which tags can the administrator configure to detect endpoints based on vulnerability severity levels? (Choose one answer)

A. Outbreak alert tags

B. Classification tags

C. Fabric tags

D. Security posture tags

Answer: D

Explanation:

According to the FortiClient EMS 7.2/7.4 Administration Guide and the ZTNA Deployment Guide, the administrator can configure Security posture tags (also known as Zero Trust Network Access (ZTNA) tags in recent versions) to detect and group endpoints based on specific compliance criteria, including vulnerability severity levels.

1. How Security Posture Tags Work for Vulnerabilities:

Tagging Rules: Under the Security Posture Tags (or Zero Trust Tags) section in EMS, an administrator creates a new rule set and adds a rule.

Rule Type: The administrator selects the Vulnerable Devices rule type.

Severity Levels: Within this rule, the administrator can specify the Severity Level (such as Critical, High, Medium, or Low). EMS dynamically applies the tag to any endpoint where the vulnerability scan detects at least one vulnerability matching or exceeding that severity level.

Dynamic Grouping: These tags allow for dynamic grouping of endpoints, which can then be synchronized with a FortiGate to enforce access control based on the device's current security posture.

2. Why Other Options are Incorrect:

A . Outbreak alert tags: While FortiGuard Outbreak alerts can be used in tagging, they specifically target endpoints vulnerable to a particular "outbreak" or high-profile threat currently active in the wild, rather than providing a general mechanism for all vulnerability severity levels.

B . Classification tags: These tags are typically used for broader endpoint identification (like department or location) and sending information to FortiAnalyzer for reporting, rather than realtime security posture compliance based on vulnerability scans.

C . Fabric tags: "Fabric" usually refers to the integration between Fortinet devices (the Security Fabric). While tags are shared across the Fabric, the specific tags configured within EMS for endpoint detection based on posture are categorized as Security Posture/Zero Trust tags.

3. Curriculum Reference:

FortiClient EMS Administration Guide (Zero Trust Tagging Rules section): Explicitly details the "Vulnerable Devices" rule type and its severity options.

EMS Study Guide (Compliance & Vulnerability): Describes using these tags to ensure endpoints meet minimum security standards before being granted access to the network.

Question: 68

Which security attribute is verified during the SSL connection negotiation between FortiClient and FortiClient EMS to mitigate man-in-the-middle (MITM) attacks? (Choose one answer)

A. serial number (SN)

B. common name (CN)

C. location (L)

D. organization (O)

Answer: B

Explanation:

According to the FortiClient EMS Administrator Study Guide (7.2/7.4 versions) and the Fortinet Document Library regarding SSL/TLS Endpoint Communication Security, the primary attribute verified during the SSL connection negotiation to mitigate Man-in-the-Middle (MITM) attacks is the Common Name (CN).

1. SSL Connection Negotiation & MITM Mitigation

Verification Process: When FortiClient attempts to establish a Telemetry connection with the FortiClient EMS server, an SSL handshake occurs. To ensure it is communicating with the legitimate server and not a malicious interceptor (MITM), FortiClient verifies the server's certificate.

Role of the Common Name (CN): The Common Name (or the Subject Alternative Name - SAN) in the certificate must match the FQDN (Fully Qualified Domain Name) or the IP address that the client intended to connect to.

Security Enforcement: If the CN/SAN does not match the server's expected address, FortiClient will detect a discrepancy. Depending on the Invalid Certificate Action setting in the profile (e.g., Warn or Block), it will prevent the establishment of a secure session to stop the MITM attacker from masquerading as the EMS server.

2. Why Other Options are Incorrect/Secondary

A . Serial Number (SN): While every certificate has a unique Serial Number, it is primarily used by the Certificate Authority (CA) for tracking and revocation purposes. While FortiOS 7.2.4+ can use SN for certain restricted VPN checks, the core SSL

negotiation mechanism for identifying a specific host to prevent spoofing relies on the CN/SAN fields.

C . Location (L) and D. Organization (O): These are descriptive fields within the certificate's Subject that provide geographical and corporate information. They are not functionally used by the SSL/TLS protocol to verify the identity of the host during the connection negotiation or to mitigate MITM attacks.

3. Curriculum Reference

EMS Administration Guide (System Settings Profile): Details how the client verifies the EMS server certificate. It specifies that for a connection to be trusted, the server address must align with the certificate's identity fields (CN/SAN).

FortiGate/FortiOS 7.2.4 New Features: Highlights the specific enhancement where FortiClient EMS connectors now "trust EMS server certificate renewals based on the CN field" to ensure continuous secure communication.