Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

NEW QUESTION 1
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: CD

Explanation:
? Understanding Multi-Tenancy Mode:
? Evaluating Benefits:
? Eliminating Incorrect Options:
References:
? FortiClient EMS multi-tenancy configuration and benefits documentation from the study guides.

NEW QUESTION 2
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.
References
? FortiClient EMS 7.2 Study Guide, FortiClient Deployment Section
? Fortinet Documentation on FortiClient Deployment using SCCM and GPO

NEW QUESTION 3
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.
References
? FortiClient EMS 7.2 Study Guide, Chromebook Management Section
? Fortinet Documentation on FortiClient EMS and Web Filtering for Chromebooks

NEW QUESTION 4
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 proxyallows 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.

References
? FortiGate Security 7.2 Study Guide, ZTNA and Proxy Configuration Sections
? Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW QUESTION 5
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

NEW QUESTION 6
Which three features does FortiClient endpoint security include? (Choose three.)

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

Answer: BDE

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

NEW QUESTION 7
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:
? Alternative Protection Features:
? Conclusion:
References:
? FortiClient web filter configuration and features from the study guides.

NEW QUESTION 8
Which component or device defines ZTNA lag information in the Security Fabric integration?

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

Answer: C

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

NEW QUESTION 9
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:
? Evaluating Deployment-2:
? Conclusion:
References:
? FortiClient EMS deployment and profile documentation from the study guides.

NEW QUESTION 10
Refer to the exhibit, which shows the output of the ZTNA traffic log on FortiGate.

```
eventtime=1633084101662546935 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=100.64.2.253 srcport=58664 srcintf="port1"
srcintfrole="wan" dstip=100.64.1.10 dstport=9443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=5215 proto=6 action="deny" policyid=0
policytype="proxy-policy" service="tcp/9443" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: failed to match a proxy-policy"
utmref=65462-14
```

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:
? Evaluating Log Message:
? Conclusion:
References:
? ZTNA traffic log analysis and configuration documentation from the study guides.

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

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

Answer: B

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

NEW QUESTION 15
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.

NEW QUESTION 16
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing. What could have caused this problem?

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

Answer: D

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

NEW QUESTION 21
Exhibit.

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

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

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

Answer: A

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

NEW QUESTION 25
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

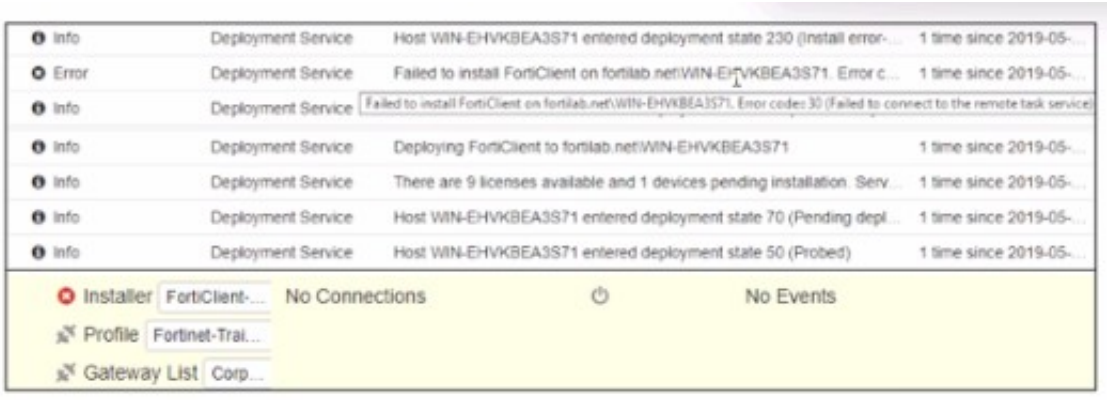
Explanation:
? Understanding Compliance Rules:
? Enforcing Compliance:
? Conclusion:
References:
? Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

NEW QUESTION 27
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

NEW QUESTION 31
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

NEW QUESTION 36
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:
? Solution Analysis:
? Evaluating Options:
? Conclusion:
References:
? FortiClient EMS and FortiGate configuration and deployment documentation from the study guides.

NEW QUESTION 39
Which component or device shares ZTNA tag information through Security Fabric integration?

A. FortiGate
B. FortiGate Access Proxy
C. FortiClient

Answer: A

Explanation:
FortiClient EMS is the component that shares ZTNA tag information through Security Fabric integration. ZTNA tags are synchronized from FortiClient EMS as inputs for the FortiGate application gateway. They can be used in ZTNA policies as security posture checks to ensure certain security criteria are met. FortiClient EMS can share ZTNA tags across multiple devices in the Fabric, such as FortiGate, FortiManager, and FortiAnalyzer. FortiClient EMS can also share ZTNA tags across multiple VDOMs on thesame FortiGate device. FortiClient EMS can be configured to control the ZTNA tag sharing behavior in the Fabric Devices settings1.
FortiGate is the device that enforces ZTNA policies using ZTNA tags. FortiGate can receive ZTNA tags from FortiClient EMS via Fabric Connector. FortiGate can also publish ZTNA services through the ZTNA portal, which allows users to access applications without installing FortiClient. FortiGate can also provide ZTNA inline CASB for SaaS application access control2.
FortiGate Access Proxy is a feature that enables FortiGate to act as a proxy for ZTNA traffic. FortiGate Access Proxy can be deployed in front of the application servers to provide ZTNA protection. FortiGate Access Proxy can also be deployed behind the application servers to provide ZTNA visibility. FortiGate Access

Proxy can use ZTNA tags to identify and authenticate users and devices2.
FortiClient is the endpoint software that connects to ZTNA services. FortiClient can register ZTNA tags with FortiClient EMS based on the endpoint security posture. FortiClient can also use ZTNA tags to access ZTNA services published by FortiGate. FortiClient can also use ZTNA tags to access SaaS applications with ZTNA inline CASB2.
References :=
? Technical Tip: Behavior of ZTNA Tags shared across multiple vdoms or multiple FortiGate firewalls in the Security Fabric connected to the same FortiClient EMS Server
? Synchronizing FortiClient ZTNA tags
? Zero Trust Network Access (ZTNA) to Control Application Access

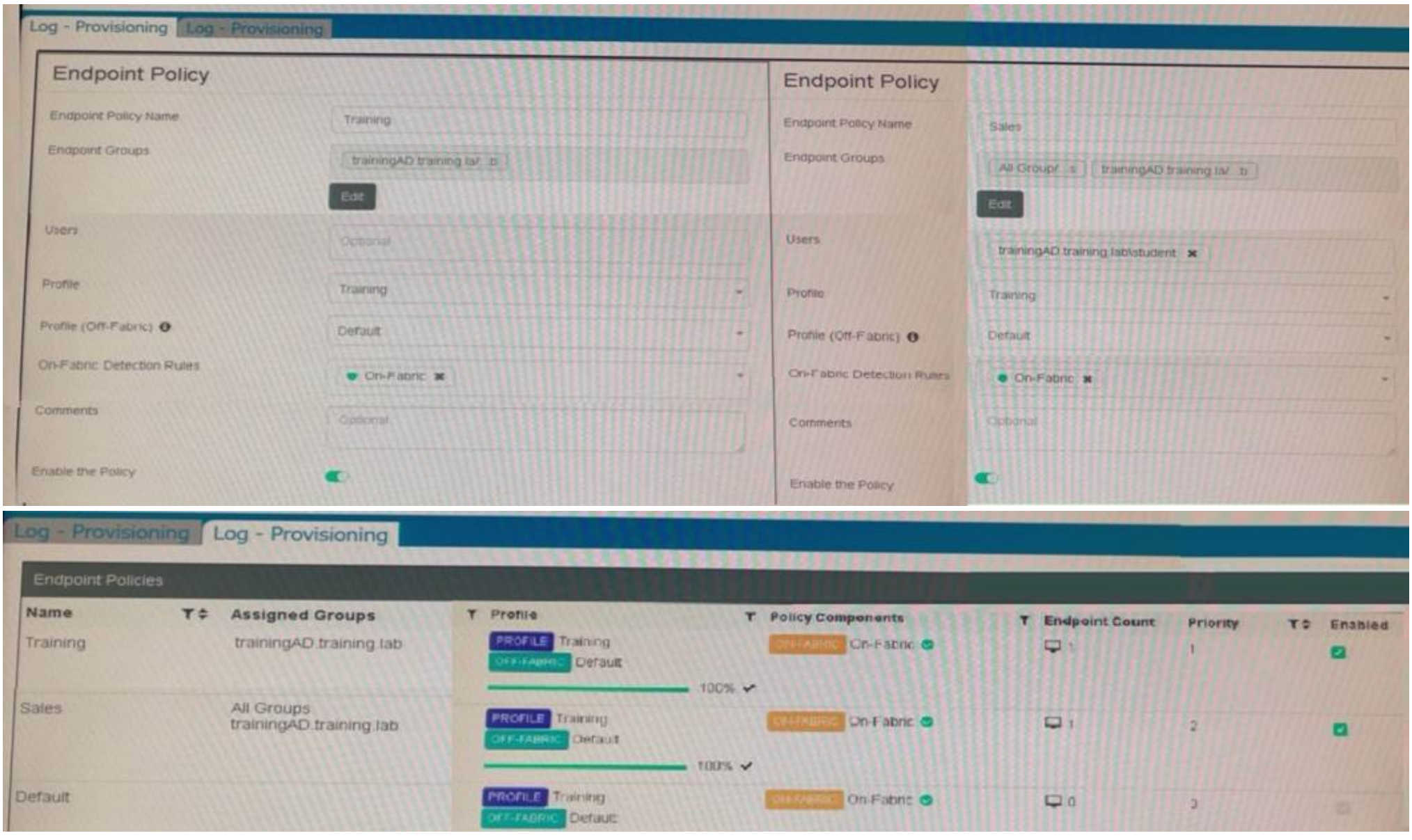
NEW QUESTION 42
An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate What is the prerequisite to get FortiClient EMS lo connect to FortiGate successfully?

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:
? Prerequisites for Connection:
? Conclusion:
References:
? FortiClient EMS and FortiGate connection and certificate management documentation from the study guides.

NEW QUESTION 45
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. References
? FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section
? FortiClient EMS Documentation on Group Policy Assignment and Matching

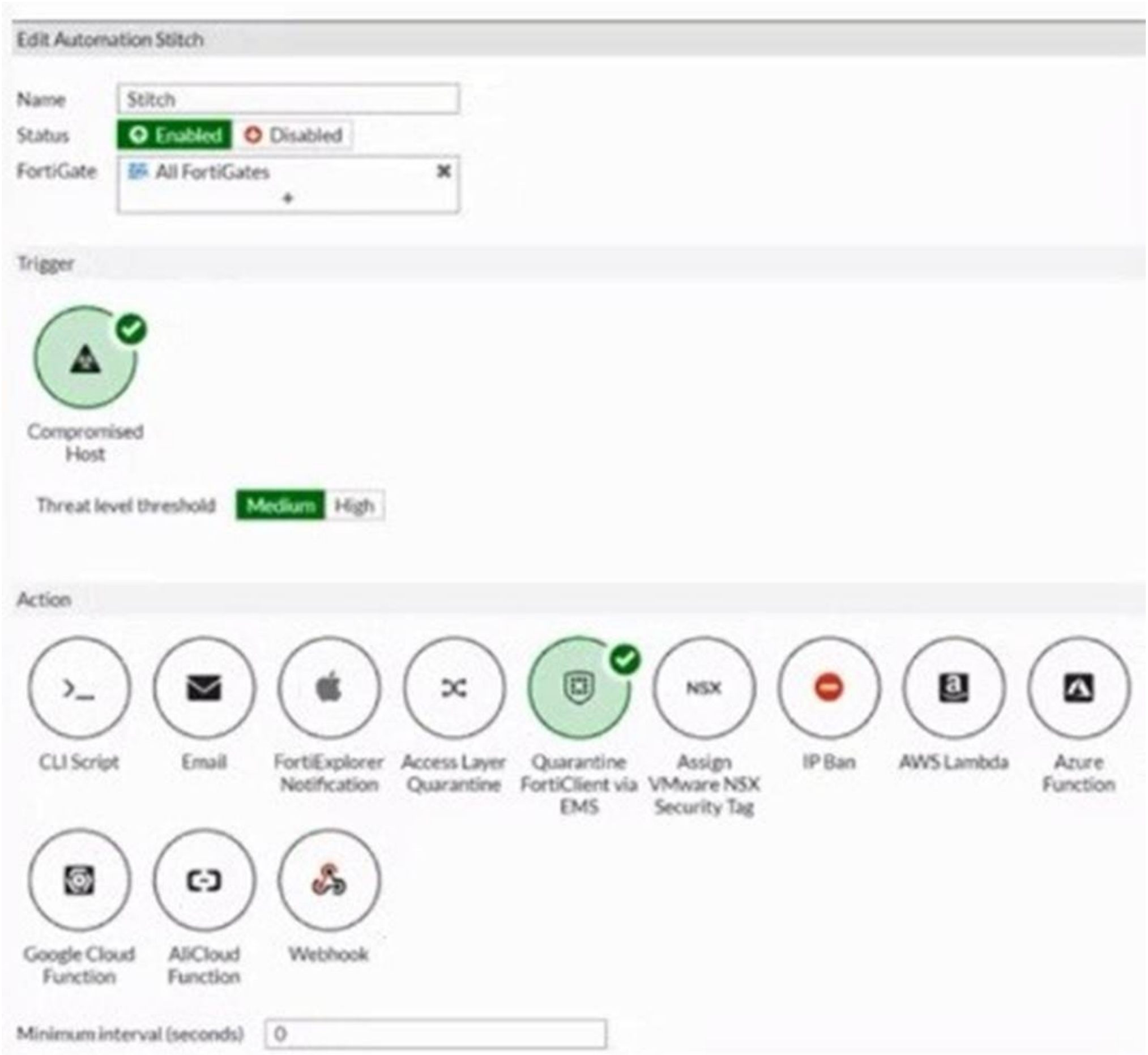
NEW QUESTION 47
Which three types of antivirus scans are available on FortiClient? (Choose three)

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

Answer: BCE

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

NEW QUESTION 52
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.
References
? FortiGate Security 7.2 Study Guide, Automation Stitches and Actions Section
? Fortinet Documentation on Configuring Automation Stitches and Quarantine Actions

NEW QUESTION 57
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:
? Evaluating Access Control Methods:
? Conclusion:
References:
? ZTNA section in the FortiGate Infrastructure 7.2 Study Guide.

NEW QUESTION 61
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FCT_AD-7.2 Practice Exam Features:

* FCP_FCT_AD-7.2 Questions and Answers Updated Frequently

* FCP_FCT_AD-7.2 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FCT_AD-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FCT_AD-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year