Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

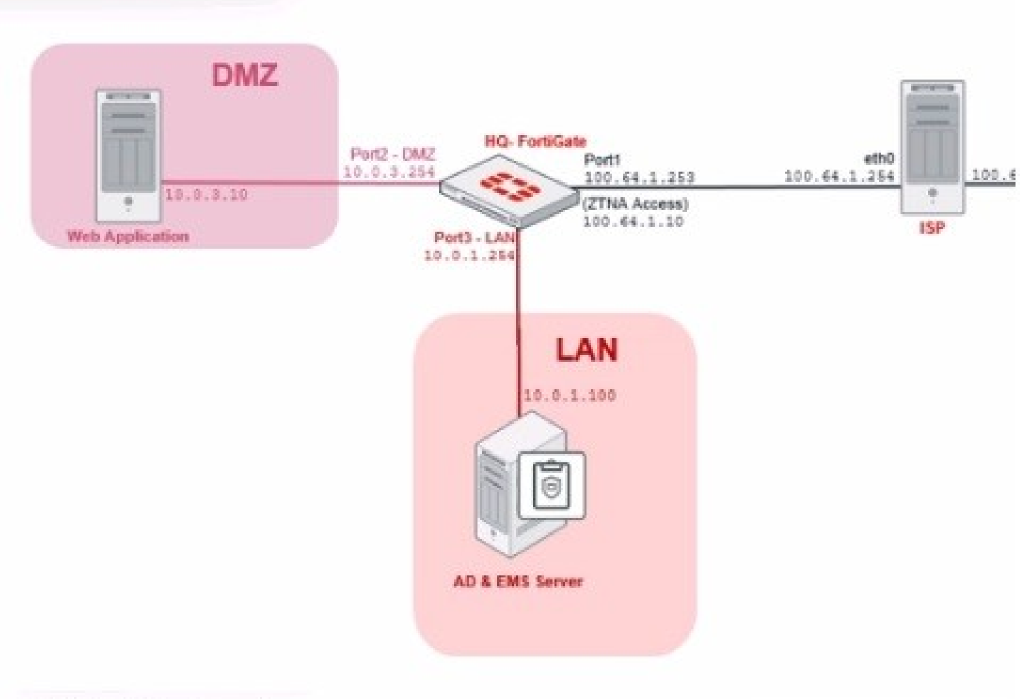
NEW QUESTION 1
Which two statements are true about the ZTNA rule? (Choose two.)

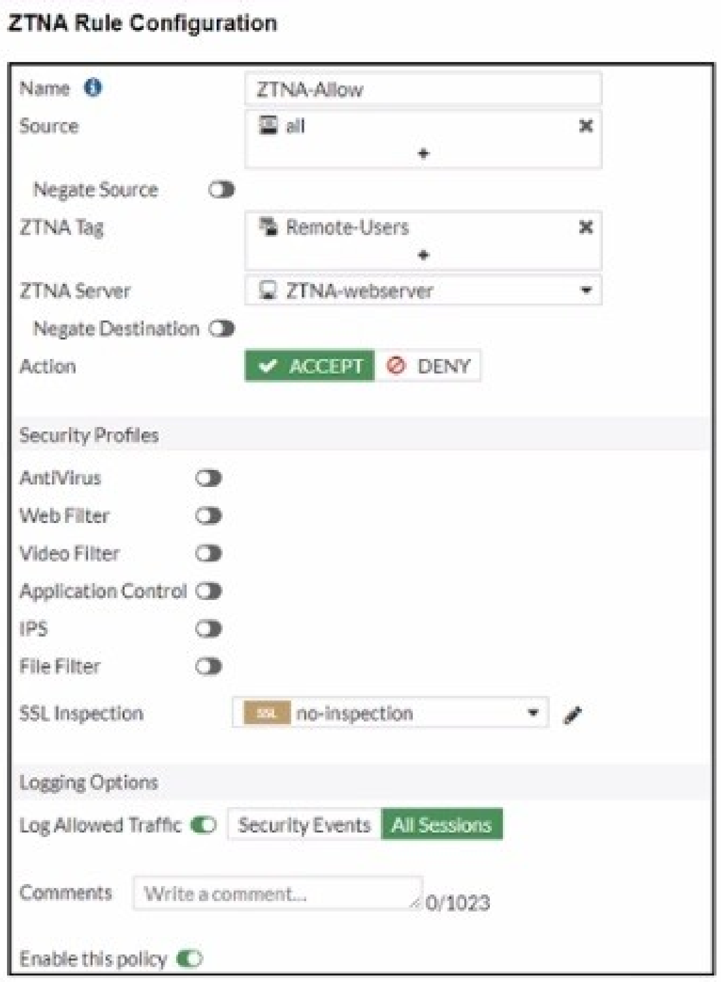
A. It applies security profiles to protect traffic
B. It applies SNAT to protect traffic.
C. It defines the access proxy.
D. It enforces access control.

Answer: AD

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

NEW QUESTION 2
ZTNA Network Topology




ZTNA Rule Configuration

Name	ZTNA-Allow
Source	all
Negate Source	○
ZTNA Tag	Remote-Users
ZTNA Server	ZTNA-webserver
Negate Destination	○
Action	✓ ACCEPT ⊘ DENY
Security Profiles	
AntiVirus	○
Web Filter	○
Video Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL no-inspection
Logging Options	
Log Allowed Traffic ●	Security Events **All Sessions**
Comments	Write a comment... 0/1023
Enable this policy ●	

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 Remote-Client 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

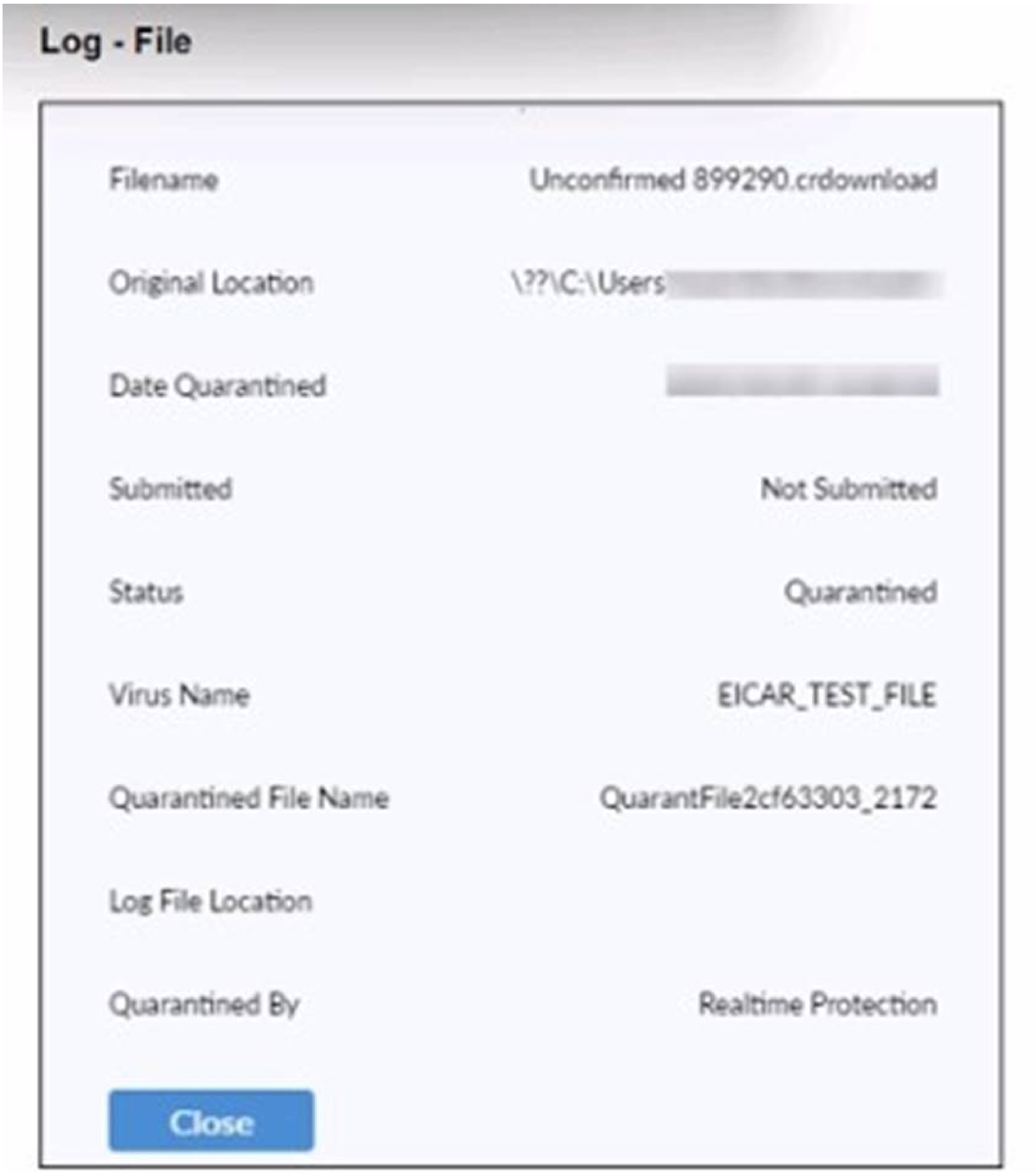
NEW QUESTION 3
An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?

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 4
Refer to the exhibit.



Log - File

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

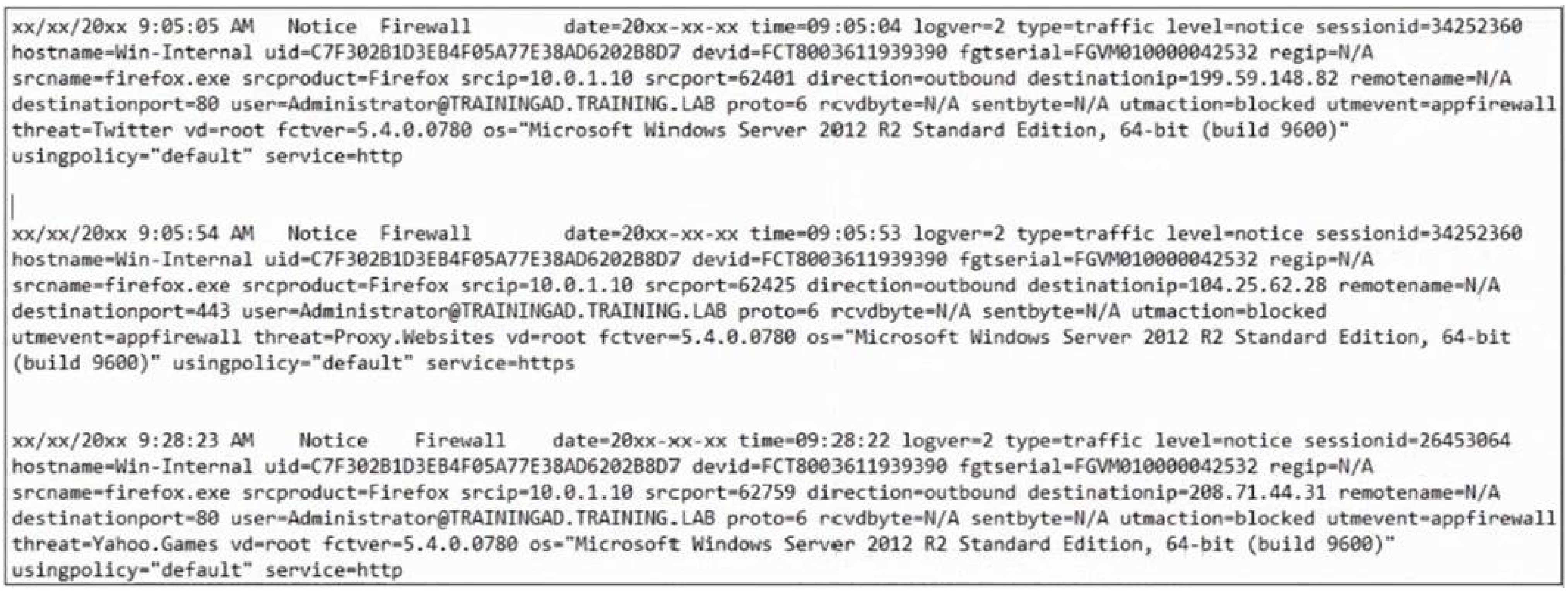
Based on the FortiClient tog details shown in the exhibit, which two statements ace true? (Choose two.)

A. The filename Is Unconfirmed 899290.crdovnload.

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

Answer: AB

NEW QUESTION 5
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 uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 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 user=Administrator@TRAININGAD.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

|
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=C7F302B1D3EB4F05A77E38AD6202B8D7 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=Administrator@TRAININGAD.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 uid=C7F302B1D3EB4F05A77E38AD6202B8D7 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=Administrator@TRAININGAD.TRAINING.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.
References
? FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section
? Fortinet Documentation on Interpreting FortiClient Logs

NEW QUESTION 6
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:
? Evaluating Options:
? Conclusion:
References:
? FortiClient EMS feature configuration and management 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?

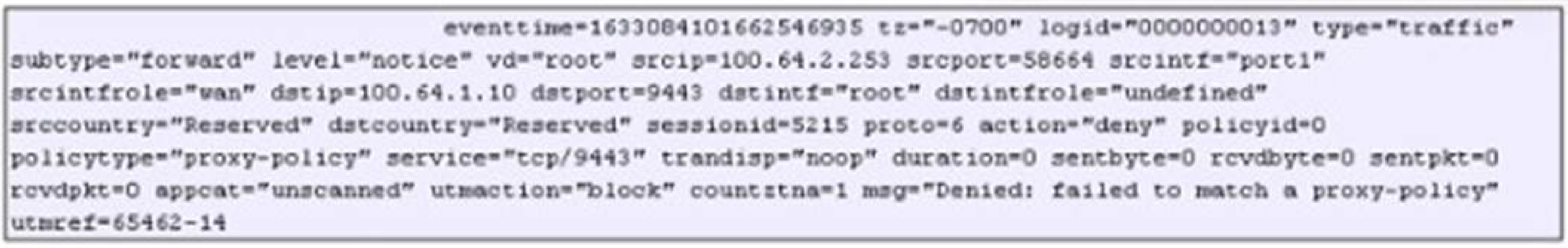
A. Real-time protection list
B. Block malicious websites on antivirus
C. FortiSandbox URL list
D. Web exclusion list

Answer: D

Explanation:
? Web Filter Functionality:
? Alternative Protection Features:

? Conclusion:
References:
? FortiClient web filter configuration and features from the study guides.

NEW QUESTION 8
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 9
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:
? Evaluating Remediation Options:
? Conclusion:
References:
? FortiSandbox integration documentation from the study guides.

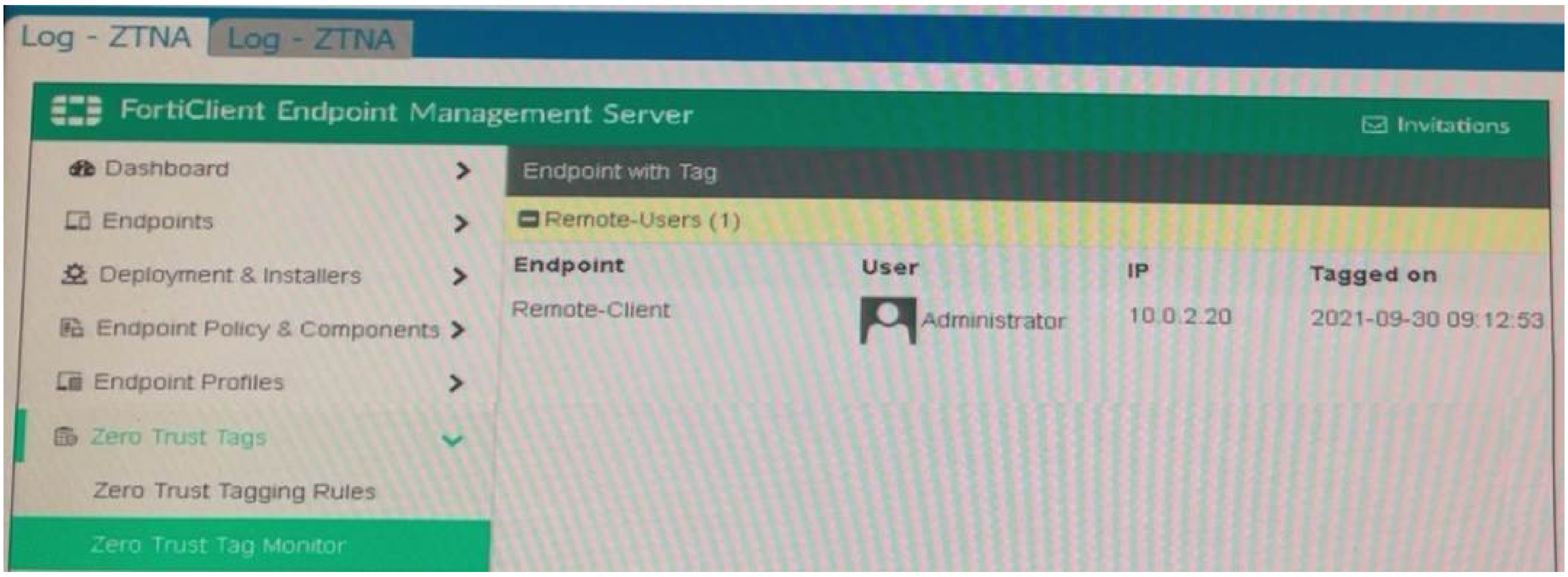
NEW QUESTION 10
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.
What could have caused this problem?

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

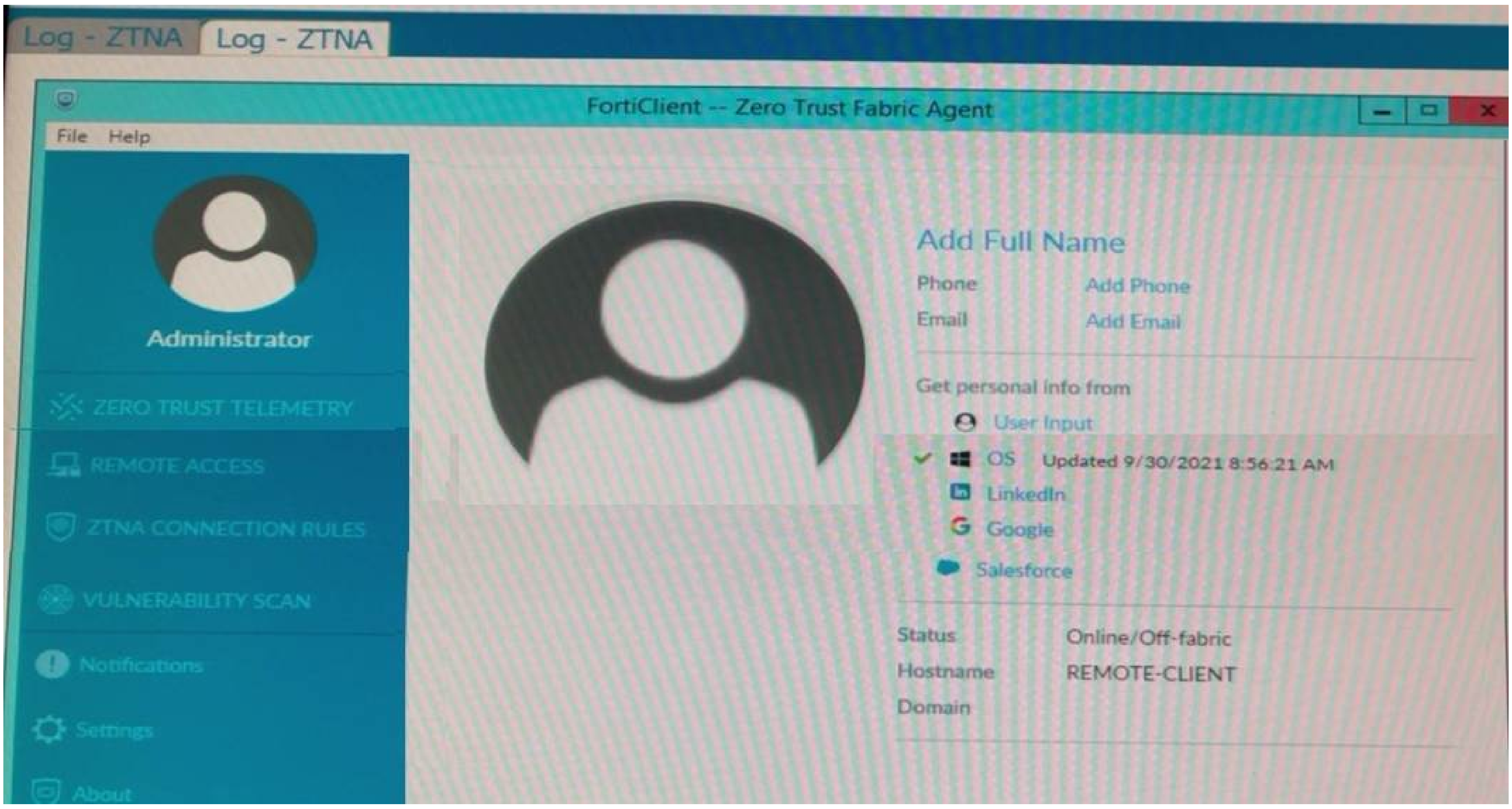
NEW QUESTION 10
Refer to the exhibits.



Endpoint with Tag

Remote-Users (1)

Endpoint	User	IP	Tagged on
Remote-Client	Administrator	10.0.2.20	2021-09-30 09:12:53



Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

User Input

✓ OS Updated 9/30/2021 8:56:21 AM

LinkedIn

Google

Salesforce

Status Online/Off-fabric

Hostname REMOTE-CLIENT

Domain

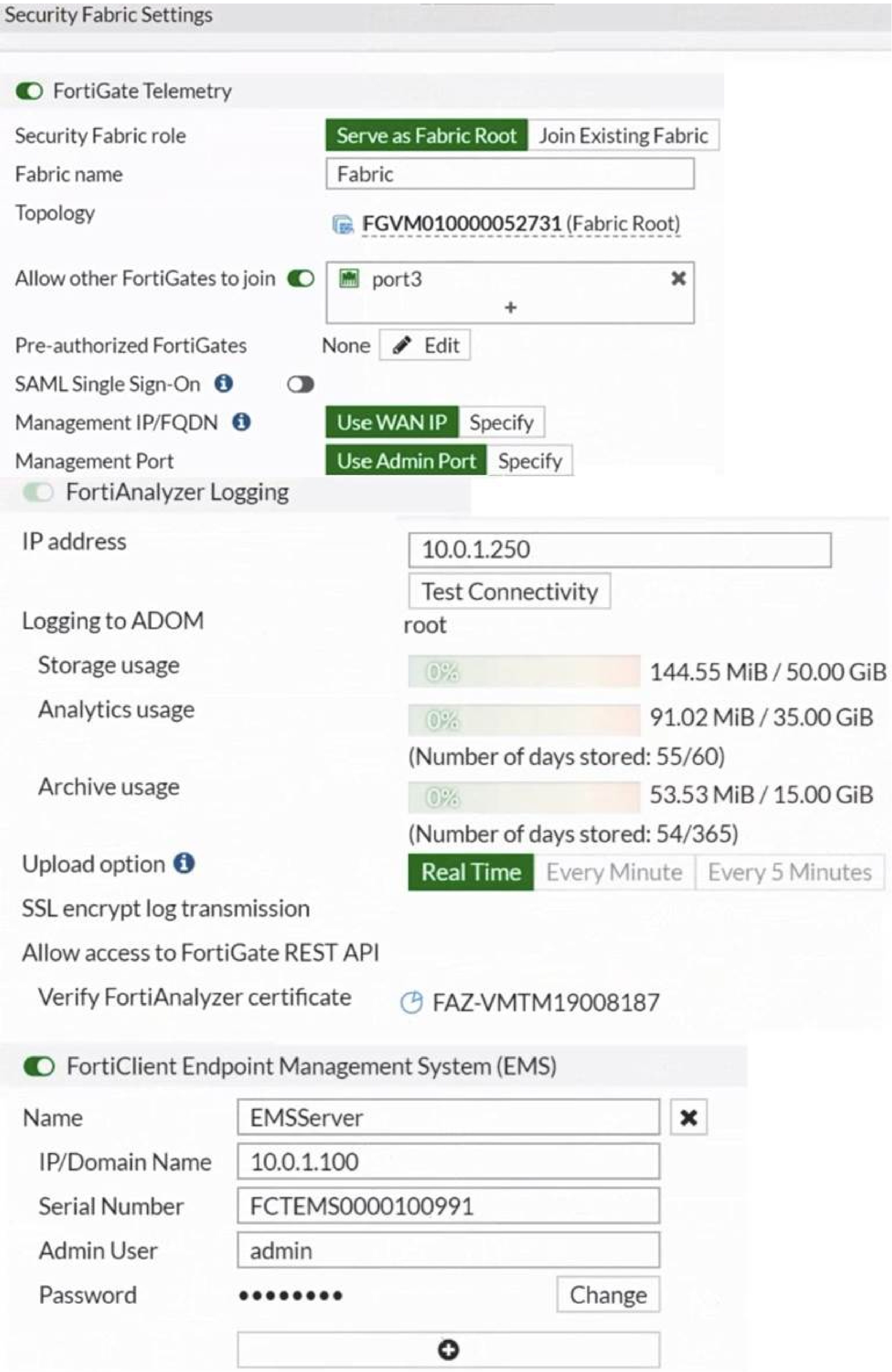
Which show the Zero Trust Tag Monitor and the FortiClient GUI status.
Remote-Client is tagged as Remote-Users on the FortiClient EMS Zero Trust Tag Monitor. What must an administrator do to show the tag on the FortiClient GUI?

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.
References
? FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Section
? FortiClient Documentation on Tag Management and Visibility Settings

NEW QUESTION 13
Refer to the exhibits.



Security Fabric Settings

FortiGate Telemetry

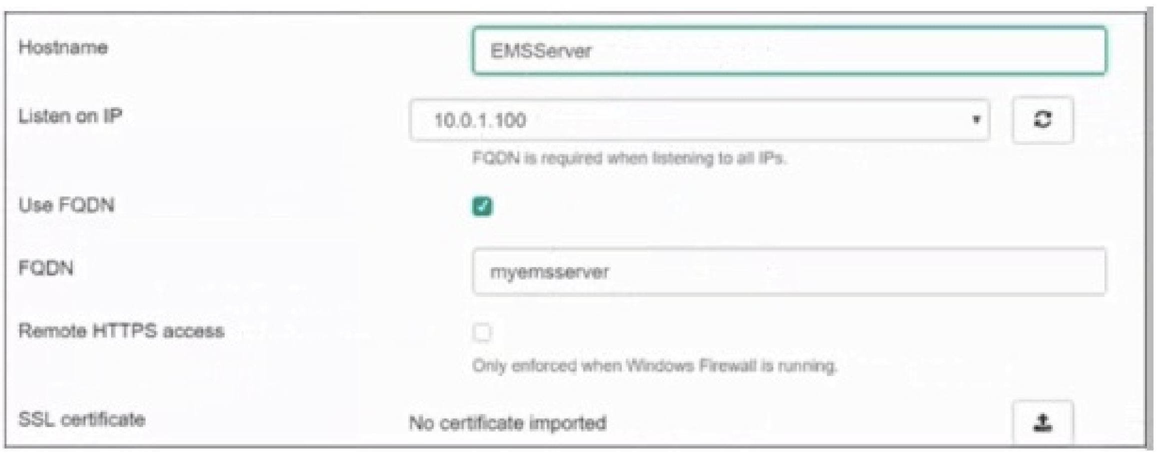
Security Fabric role	[✓ Serve as Fabric Root] Join Existing Fabric
Fabric name	Fabric
Topology	FGVM010000052731 (Fabric Root)
Allow other FortiGates to join	port3
Pre-authorized FortiGates	None Edit
SAML Single Sign-On	
Management IP/FQDN	[✓ Use WAN IP] Specify
Management Port	[✓ Use Admin Port] Specify

FortiAnalyzer Logging

IP address	10.0.1.250 Test Connectivity
Logging to ADOM	root
Storage usage	0% 144.55 MiB / 50.00 GiB
Analytics usage	0% 91.02 MiB / 35.00 GiB (Number of days stored: 55/60)
Archive usage	0% 53.53 MiB / 15.00 GiB (Number of days stored: 54/365)
Upload option	[✓ Real Time] Every Minute Every 5 Minutes
SSL encrypt log transmission	
Allow access to FortiGate REST API	
Verify FortiAnalyzer certificate	FAZ-VMTM19008187

FortiClient Endpoint Management System (EMS)

Name	EMSServer
IP/Domain Name	10.0.1.100
Serial Number	FCTEMS0000100991
Admin User	admin
Password	••••••••• Change



Hostname	EMSServer
Listen on IP	10.0.1.100 FQDN is required when listening to all IPs.
Use FQDN	☑
FQDN	myemsserver
Remote HTTPS access	□ Only enforced when Windows Firewall is running.
SSL certificate	No certificate imported

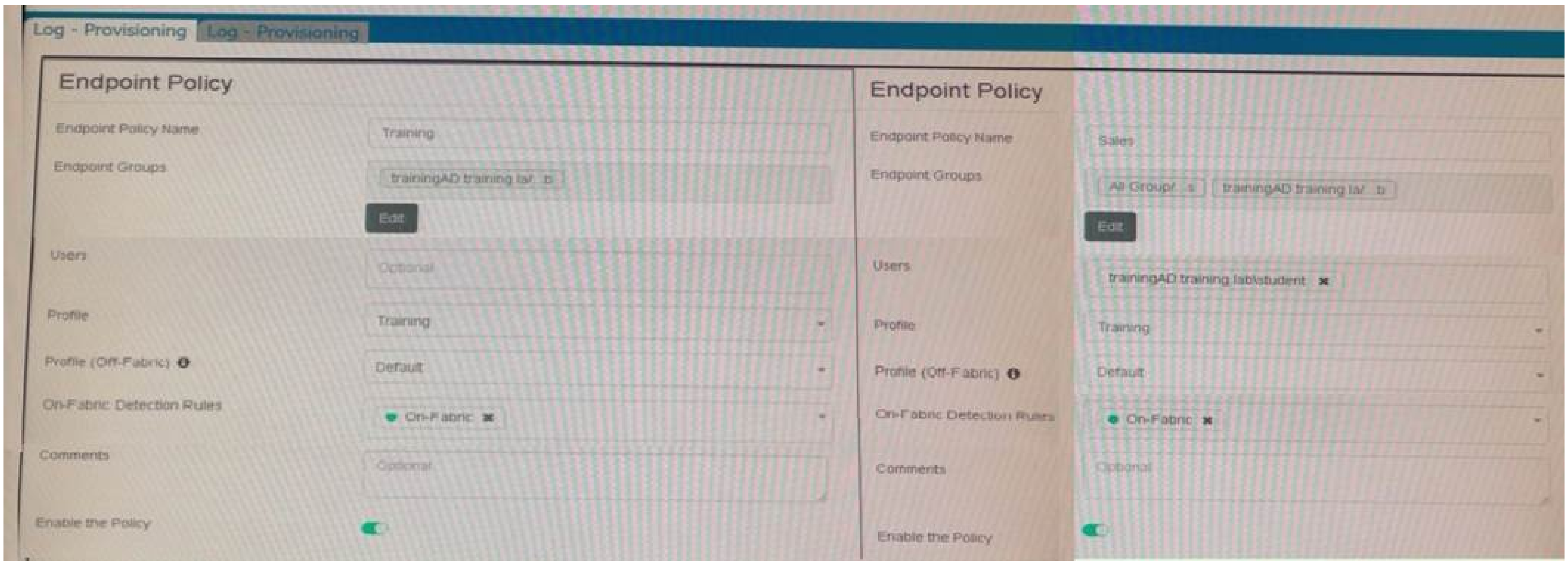
Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint. when it is detected as a compromised host (loC)?

A. The administrator must enable remote HTTPS access to EMS.
B. The administrator must enable FQDN on EMS.
C. The administrator must authorize FortiGate on FortiAnalyzer.
D. The administrator must enable SSH access to EMS.

Answer: A

Explanation:
Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:
? Enable Remote HTTPS Access to EMS:This setting allows FortiGate to
communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate.
Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.
References
? FortiGate Infrastructure 7.2 Study Guide, Security Fabric and Integration with EMS Sections
? Fortinet Documentation on Enabling Remote HTTPS Access to FortiClient EMS

NEW QUESTION 17
Refer to the exhibits.

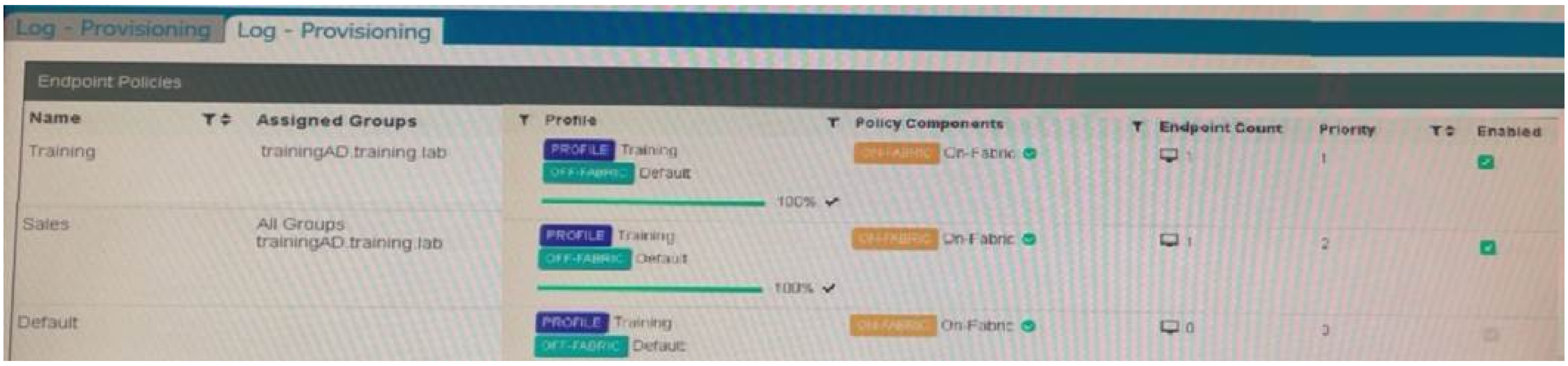


Endpoint Policy

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

Endpoint Policy

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



Endpoint Policies

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

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

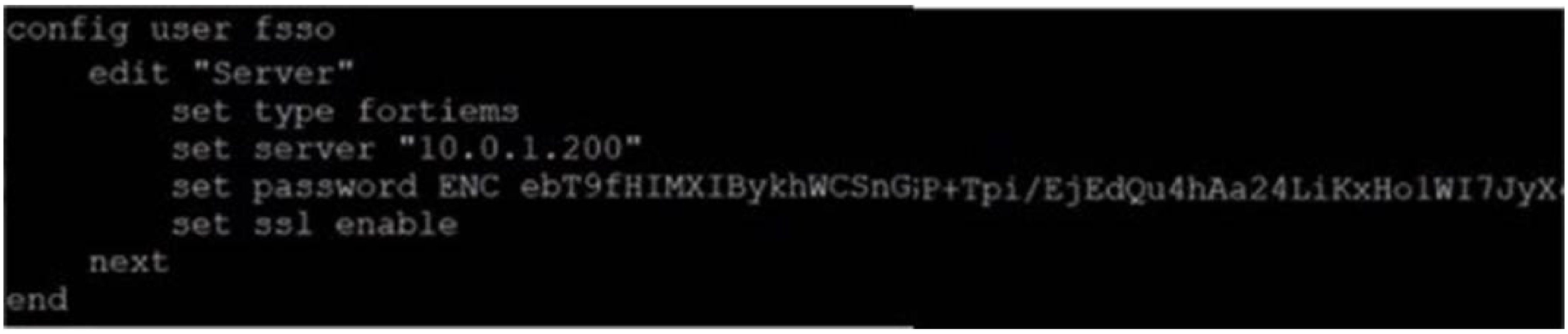
A. FortiClient EMS will assign the Sales policy
B. FortiClient EMS will assign the Training policy
C. FortiClient EMS will assign the Default policy
D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Answer: B

Explanation:
Based on the configuration shown in the exhibits:

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

NEW QUESTION 21
Refer to the exhibit.



```
config user fsso
    edit "Server"
        set type fortiems
        set server "10.0.1.200"
        set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHolWI7JyX
        set ssl enable
    next
end
```

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.
References
? FortiGate Security 7.2 Study Guide, FSSO Configuration Section
? Fortinet Documentation on FortiGate and FortiClient EMS Integration

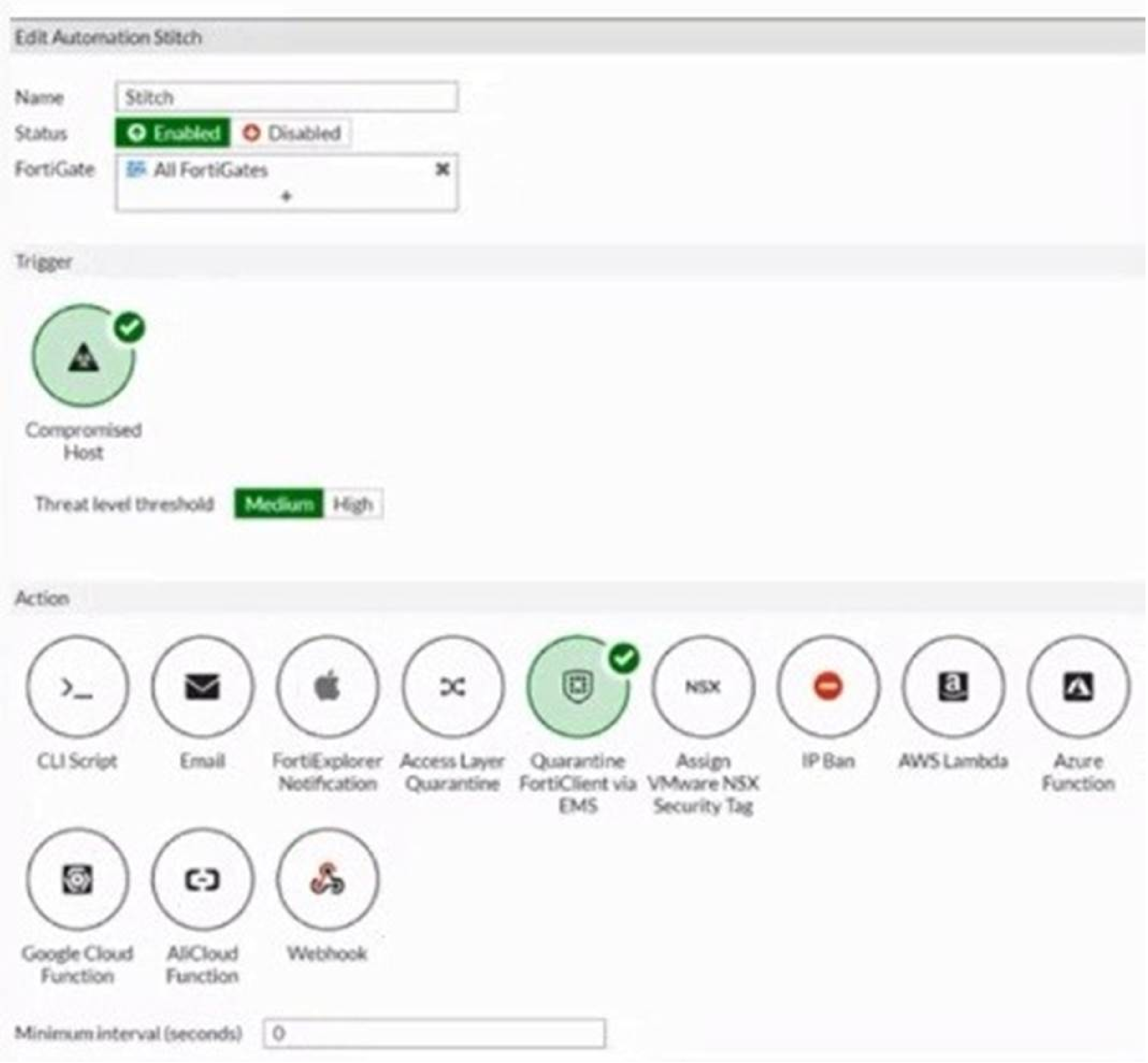
NEW QUESTION 25
Which three types of antivirus scans are available on FortiClient? (Choose three)

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 28
Refer to the exhibit.



Edit Automation Stitch

Name: Stitch

Status: Enabled | Disabled

FortiGate: All FortiGates

Trigger

Threat level threshold: Medium | High

Action

Minimum interval (seconds): 0

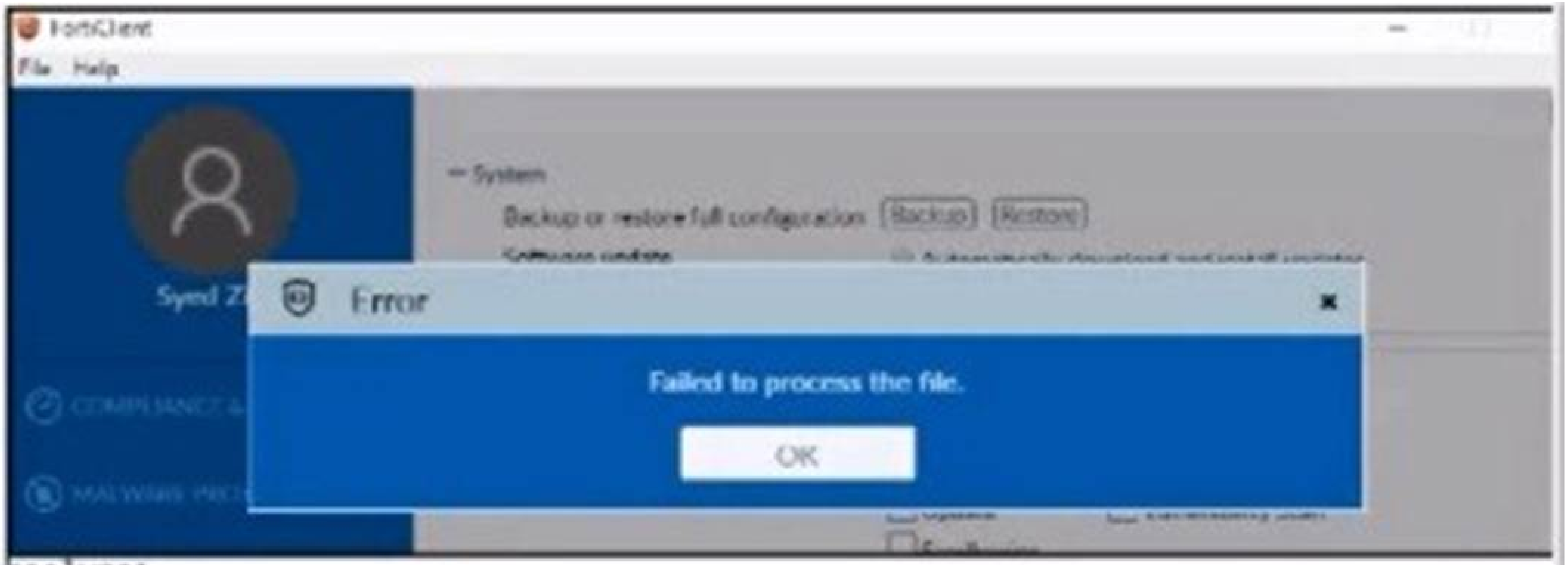
Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

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

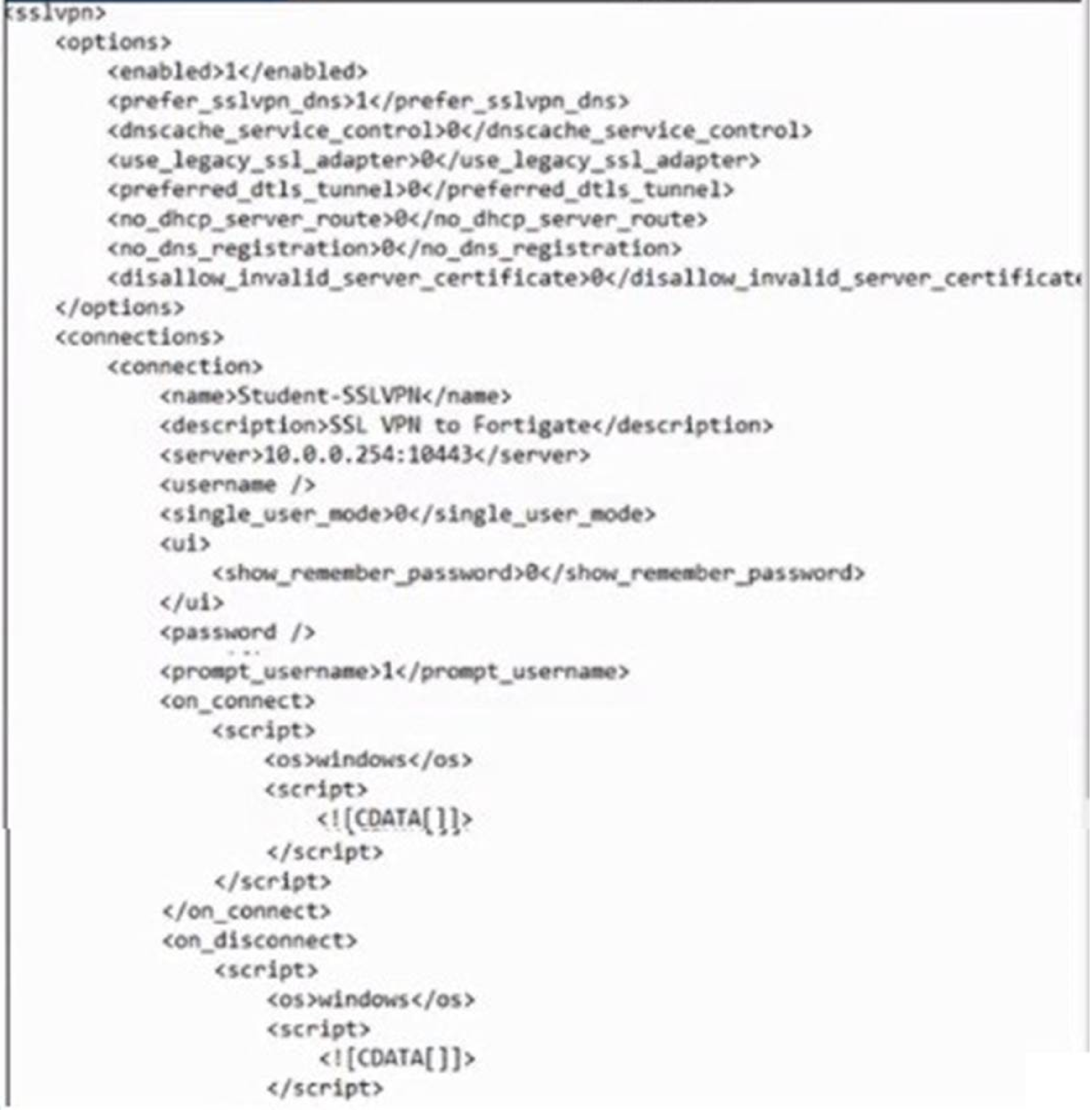
Answer: A

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

NEW QUESTION 33
Refer to the exhibit.



Failed to process the file.



```
<sslvpn>
    <options>
        <enabled>1</enabled>
        <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
        <dnscache_service_control>0</dnscache_service_control>
        <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
        <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
        <no_dhcp_server_route>0</no_dhcp_server_route>
        <no_dns_registration>0</no_dns_registration>
        <disallow_invalid_server_certificate>0</disallow_invalid_server_certificat
    </options>
    <connections>
        <connection>
            <name>Student-SSLVPN</name>
            <description>SSL VPN to Fortigate</description>
            <server>10.0.0.254:10443</server>
            <username />
            <single_user_mode>0</single_user_mode>
            <ui>
                <show_remember_password>0</show_remember_password>
            </ui>
            <password />
              ...
            <prompt_username>1</prompt_username>
            <on_connect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_connect>
            <on_disconnect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
```

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.
References
? FortiClient EMS 7.2 Study Guide, Configuration File Management Section
? General XML Syntax Guidelines and Best Practices

NEW QUESTION 34
......