Fortinet

Exam Questions FCP_FCT_AD-7.4

FCP - FortiClient EMS 7.4 Administrator

NEW QUESTION 1
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. FortiCIient ZTNA destination authentication is enabled by default.

Answer: CD

NEW QUESTION 2
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

NEW QUESTION 3
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

NEW QUESTION 4
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

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

NEW QUESTION 6
Refer to the exhibit.

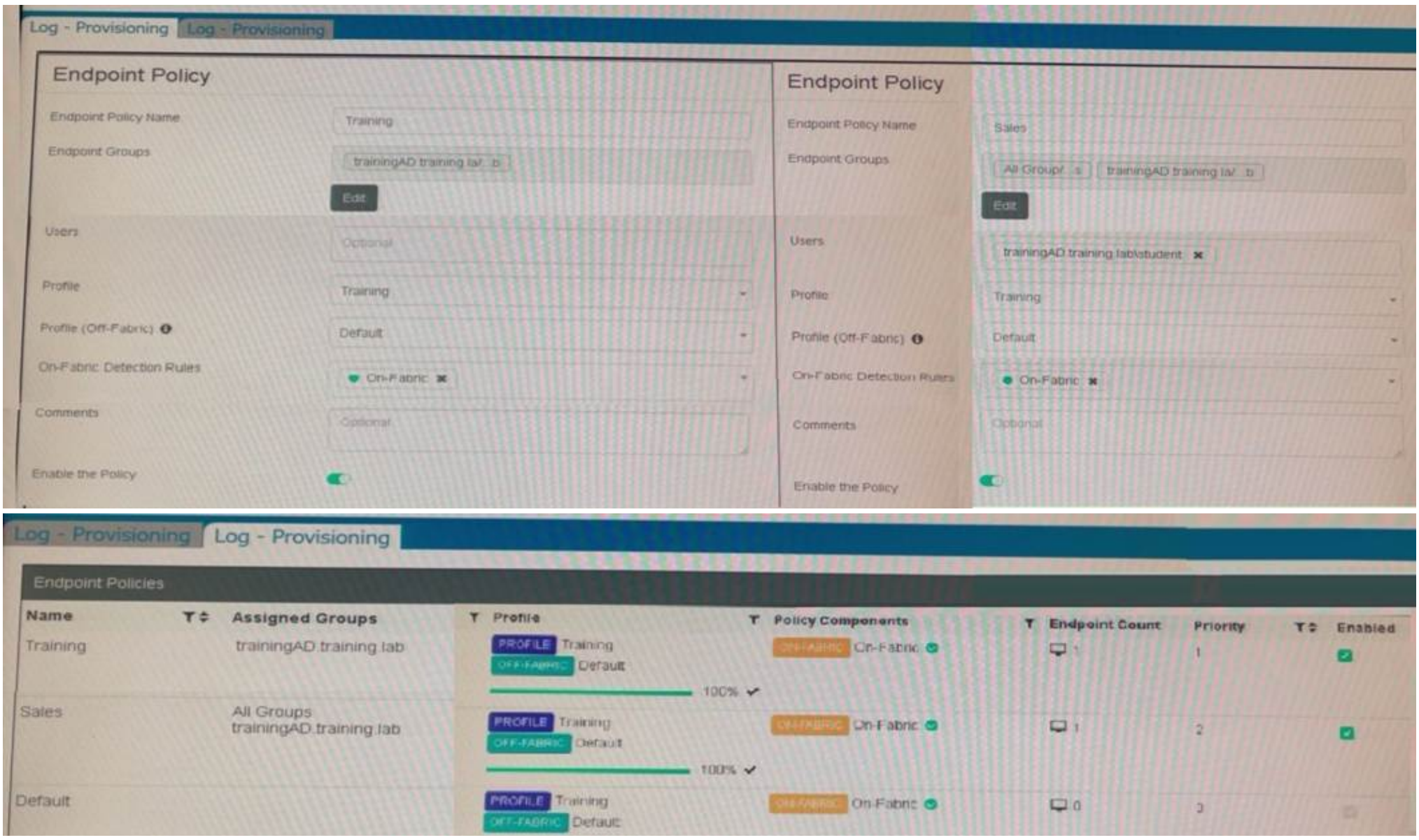
```
xx/xx/20xx 9:05:05 AM   Notice  Firewall       date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 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

NEW QUESTION 7
Refer to the exhibits.

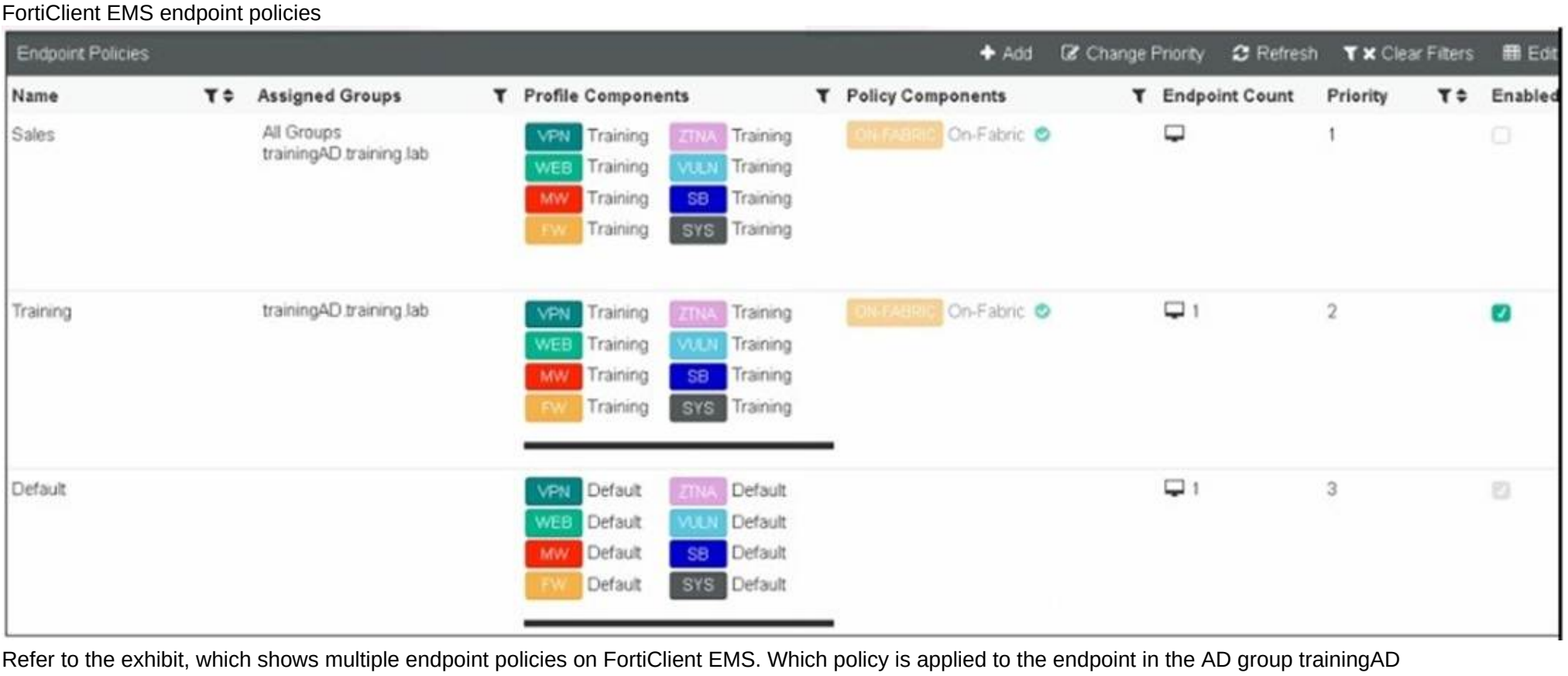


Which shows the configuration of endpoint policies.
Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

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

NEW QUESTION 8
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

NEW QUESTION 9
Refer to the exhibit.


```
<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

NEW QUESTION 10
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

NEW QUESTION 10
Which component or device shares device status information through ZTNA telemetry?

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

Answer: A

NEW QUESTION 14
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

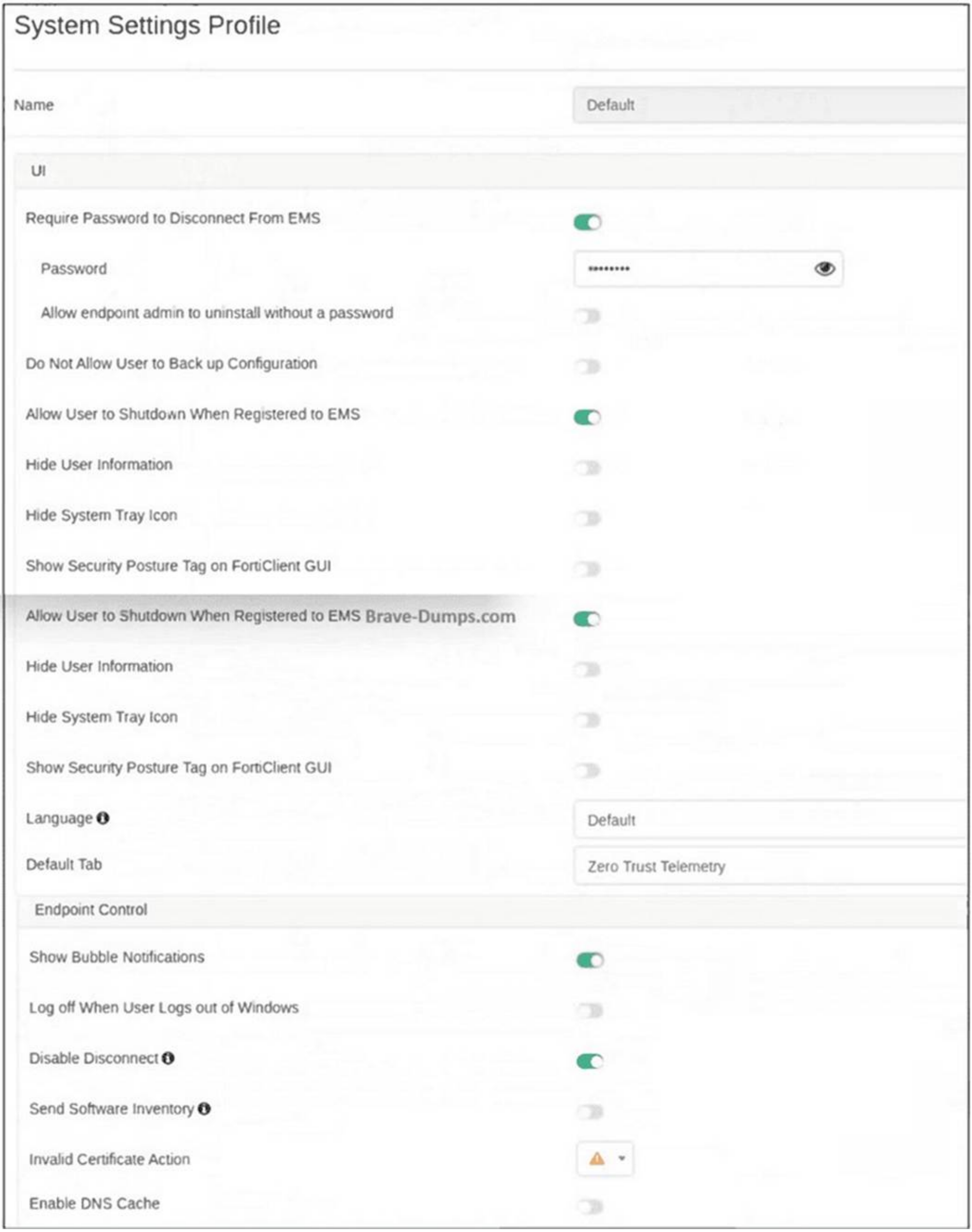
NEW QUESTION 15
A FortiClient EMS administrator is implementing additional security on FortiClient for compliance checks. Which tags can the administrator configure to detect endpoints based on vulnerability severity levels? (Choose one answer)

A. Outbreak alert tags
B. Classification tags
C. Fabric tags
D. Security posture tags

Answer: D

NEW QUESTION 18
Refer to the exhibit.

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

NEW QUESTION 22
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

NEW QUESTION 24
Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

Deployments

+ Add | Change Priority

Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
Deployment-1	All Groups	First-Time-Installation		1	☐
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade		2	☑

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

NEW QUESTION 25
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

NEW QUESTION 28
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

NEW QUESTION 31
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

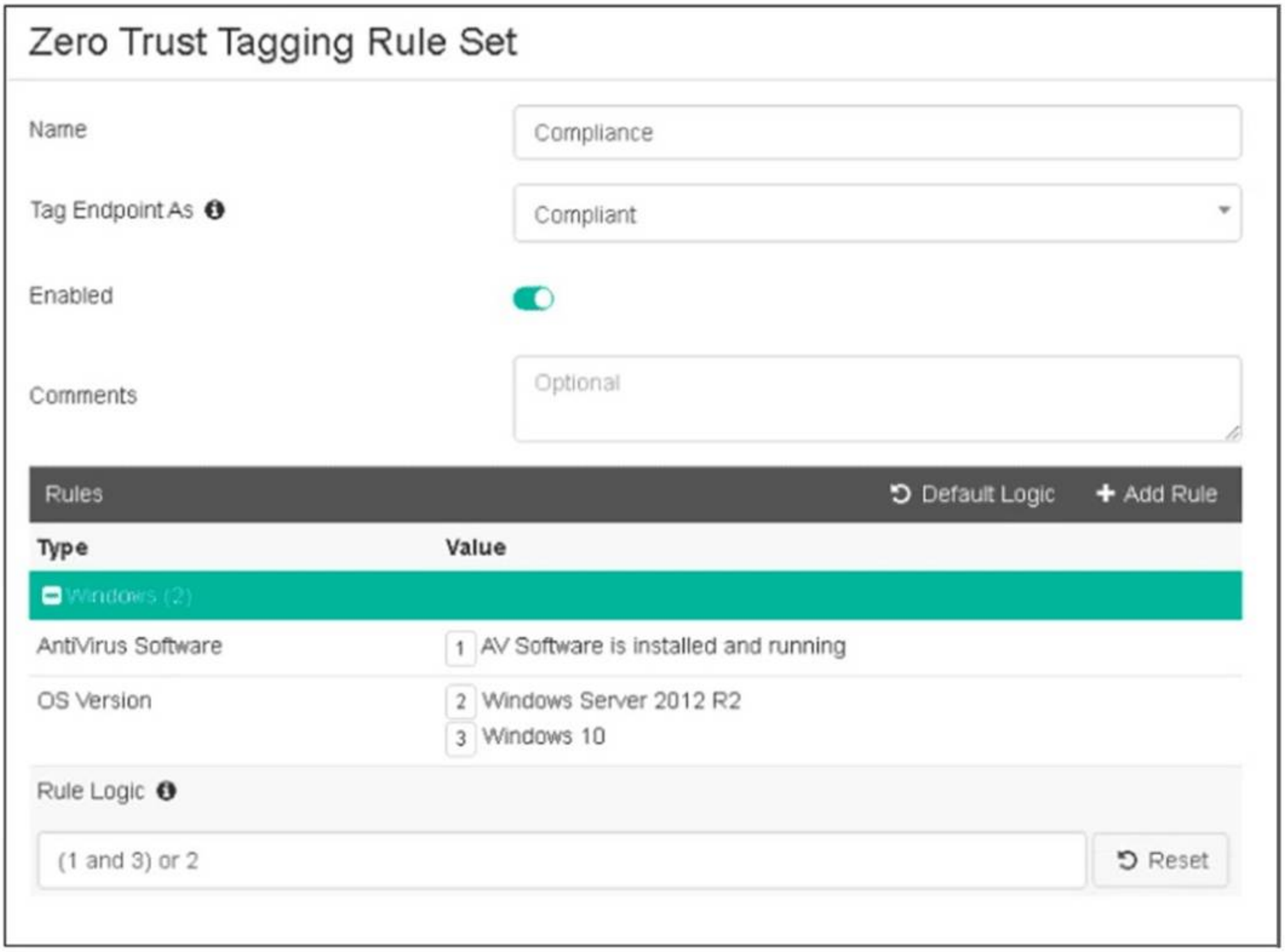
Answer: D

NEW QUESTION 36
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

NEW QUESTION 38
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

NEW 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. lt helps to safeguard systems from advanced security threats, such as malware.

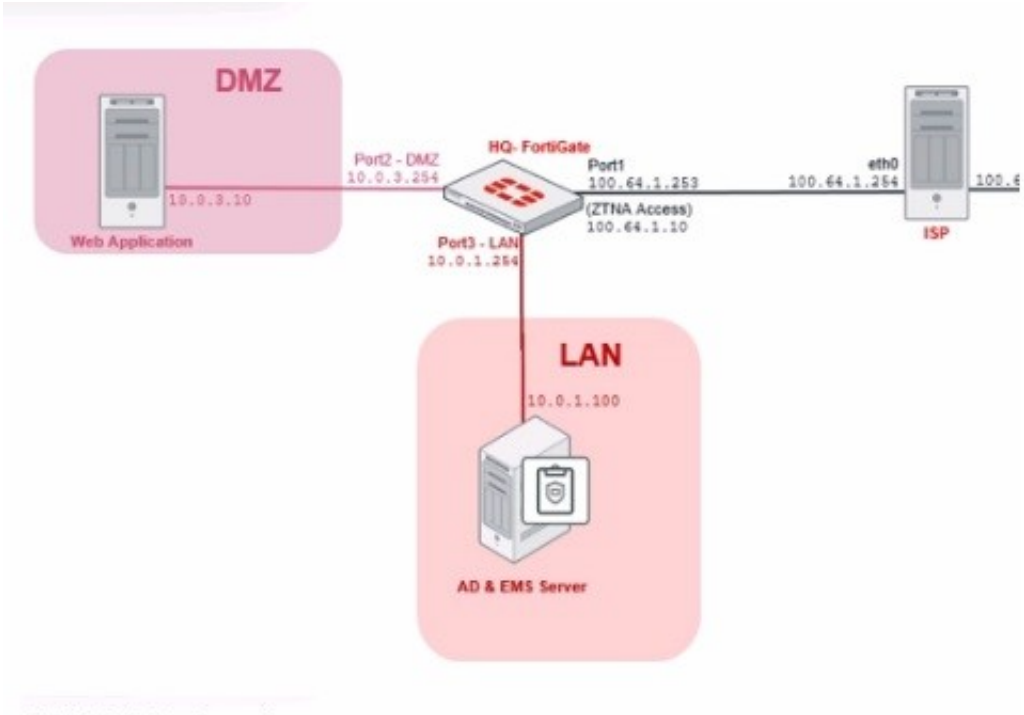
Answer: D

NEW QUESTION 47
An administrator installs FortiClient EMS in the enterprise.
Which component is responsible for enforcing protection and checking security posture?

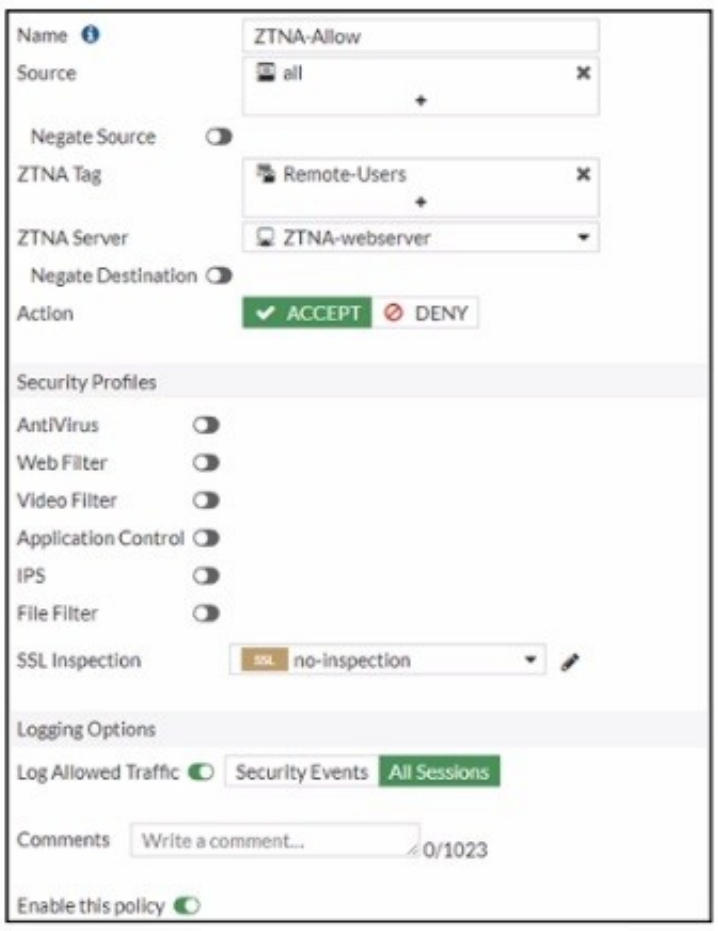
A. FortiClient EMS tags
B. FortiClient vulnerability scan
C. FortiClient
D. FortiClient EMS

Answer: C

NEW QUESTION 48
ZTNA Network Topology



ZTNA Rule Configuration



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.

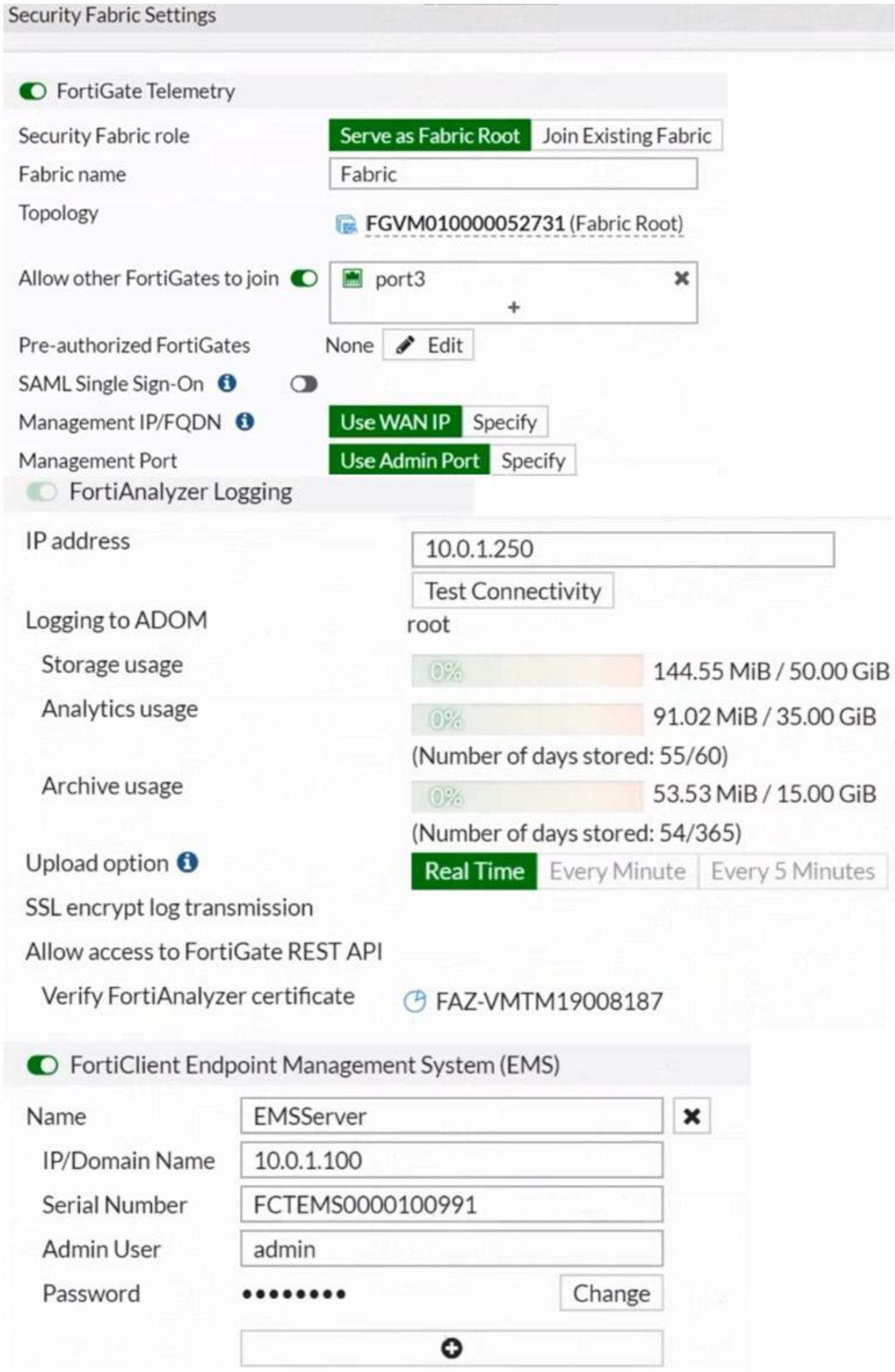
Answer: D

NEW QUESTION 49
What does FortiClient do as a fabric agent? (Choose two.)

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

Answer: CD

NEW QUESTION 50
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

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 (IoC)?

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.

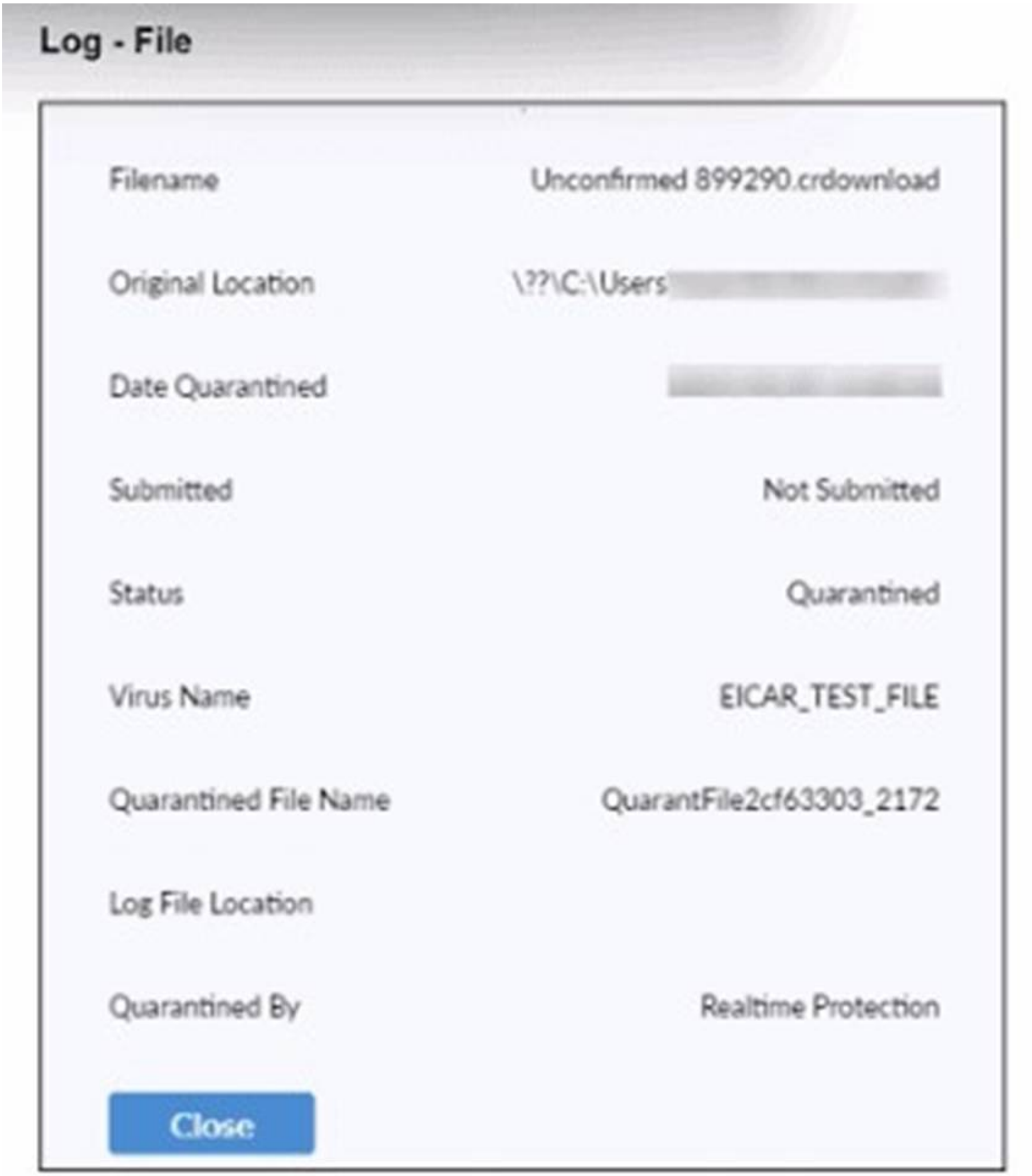
Answer: A

NEW QUESTION 53
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

NEW QUESTION 55
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

NEW QUESTION 56
Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

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

Answer: CD

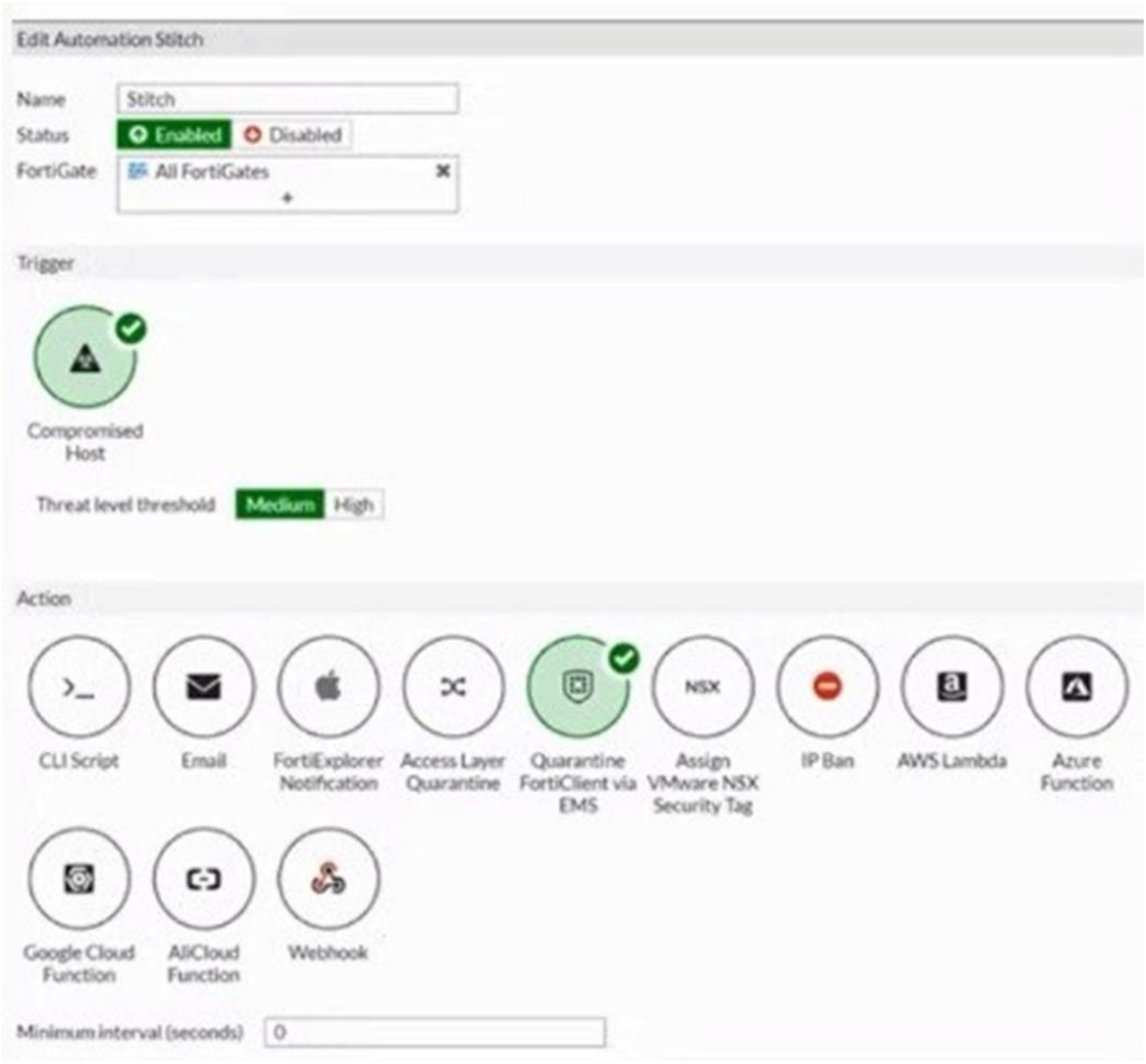
NEW QUESTION 61
A company must integrate the FortiClient EMS with their existing identity management infrastructure for user authentication, and implement and enforce

administrative access with multi-factor 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

NEW QUESTION 63
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

NEW QUESTION 66
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.

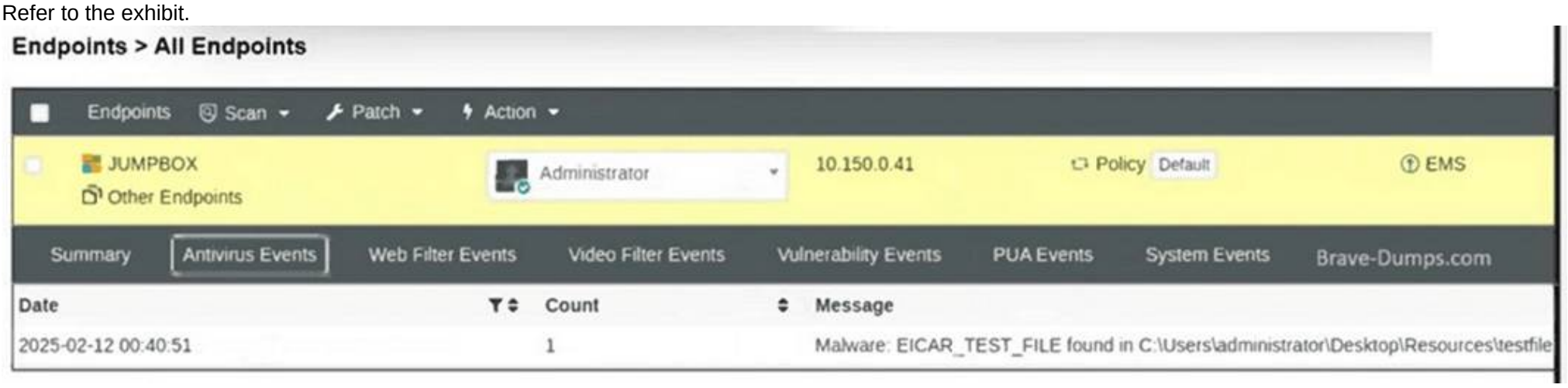
Answer: B

NEW QUESTION 71
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 file
C. DLLs, and drivers for throats.
D. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
E. It scans executable file
F. DLLs, and drivers that are currently running, for threats.

Answer: B

NEW QUESTION 76
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

NEW QUESTION 80
.....

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-7.4 Practice Exam Features:

* FCP_FCT_AD-7.4 Questions and Answers Updated Frequently

* FCP_FCT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FCT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FCT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year