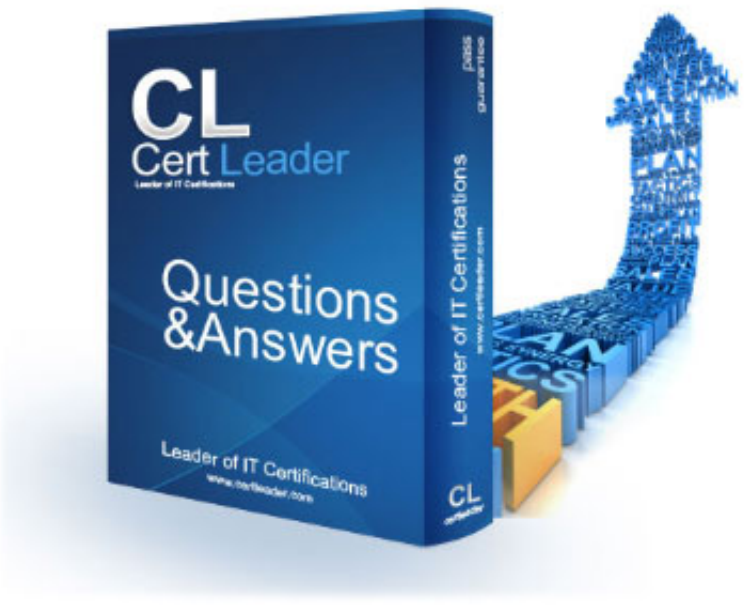
FCP_FCT_AD-7.4 Dumps

FCP - FortiClient EMS 7.4 Administrator

https://www.certleader.com/FCP_FCT_AD-7.4-dumps.html



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
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

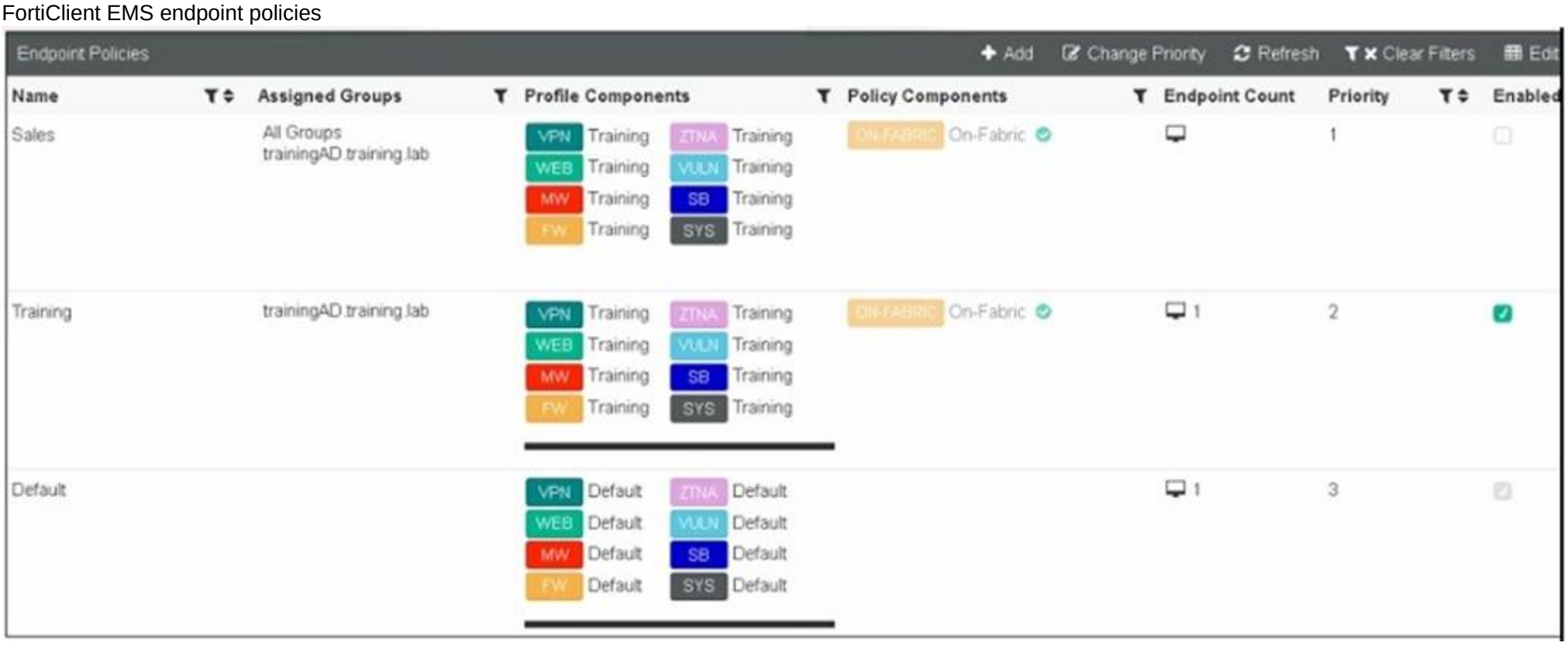
Answer: D

NEW QUESTION 4
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

NEW QUESTION 5
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

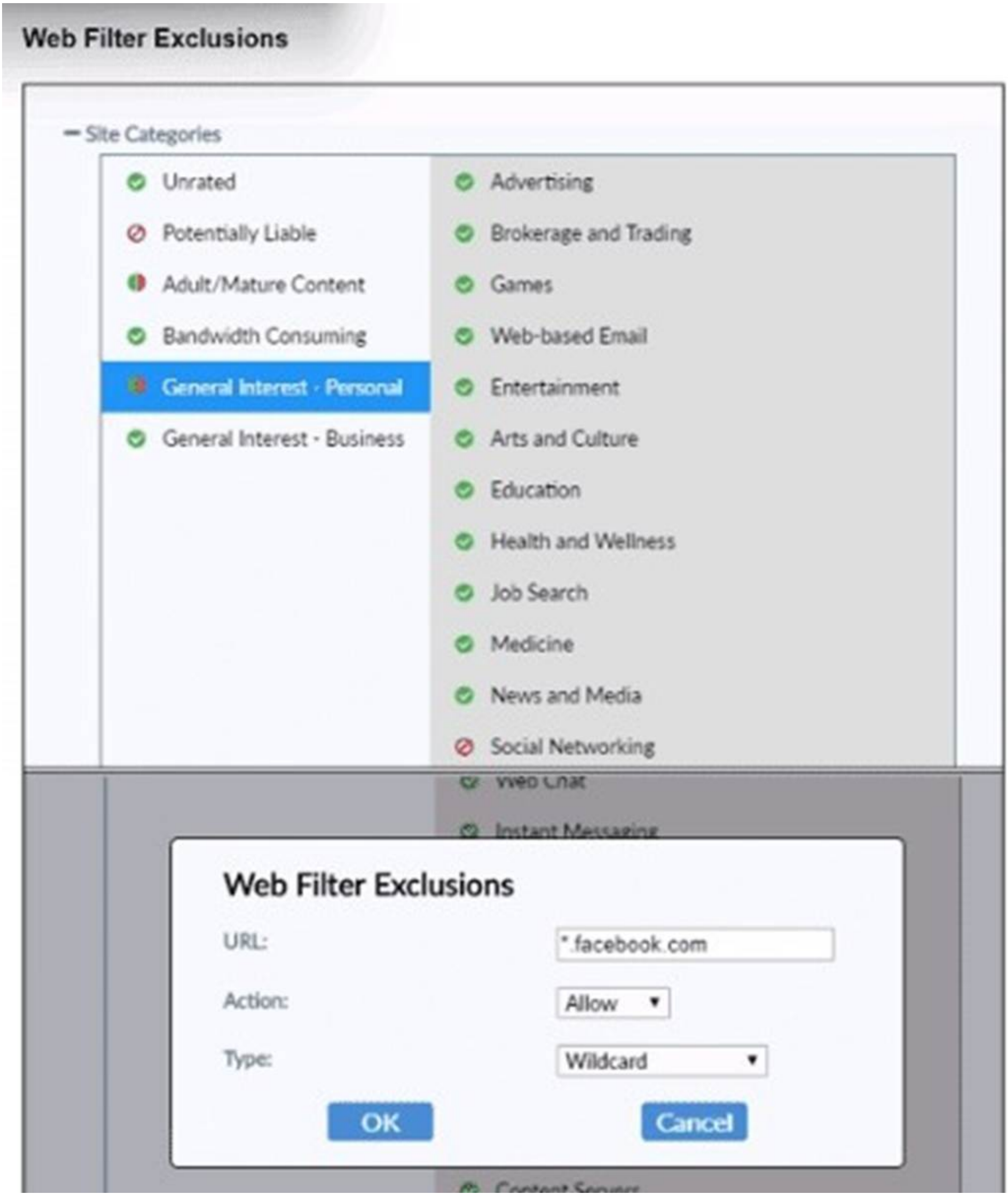
Answer: A

NEW QUESTION 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

NEW QUESTION 7
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

NEW QUESTION 8
Which component or device shares device status information through ZTNA telemetry?

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

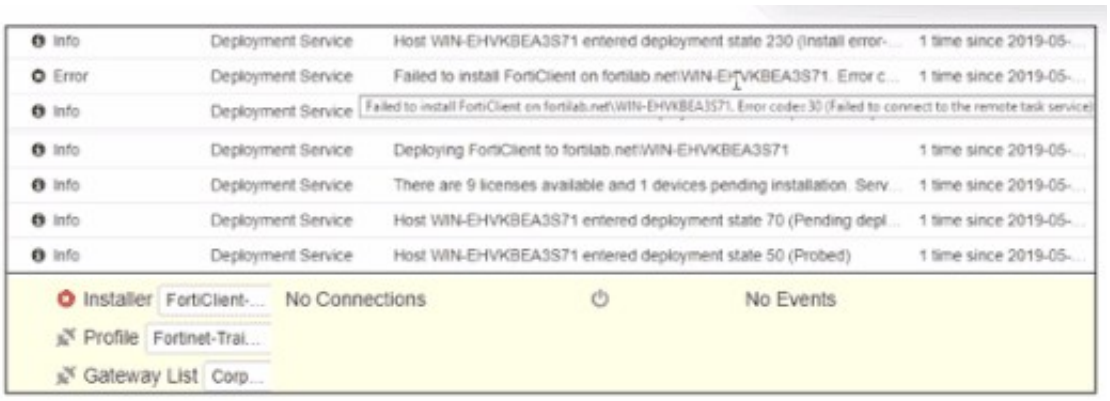
Answer: A

NEW QUESTION 9
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 10
Exhibit.

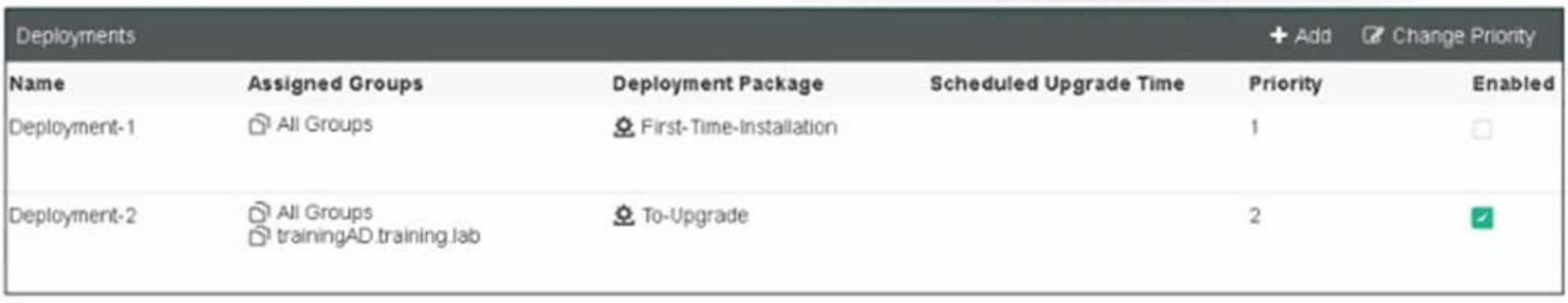


Based on the logs shown in the exhibit, why did FortiClient EMS tail to install FortiClient on the endpoint?

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

NEW QUESTION 10
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

NEW QUESTION 14
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

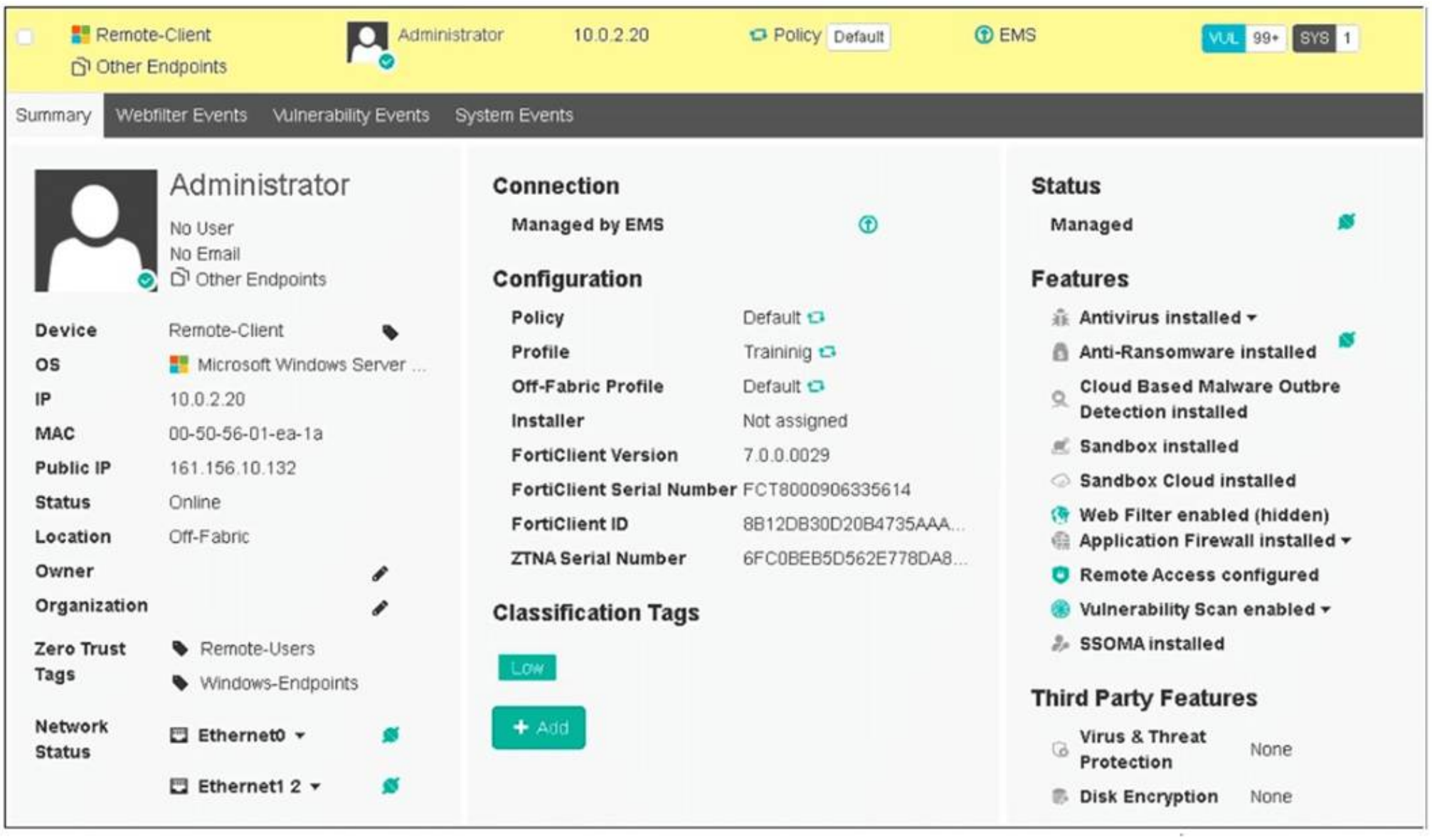
Answer: C

NEW QUESTION 19
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 23
Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.

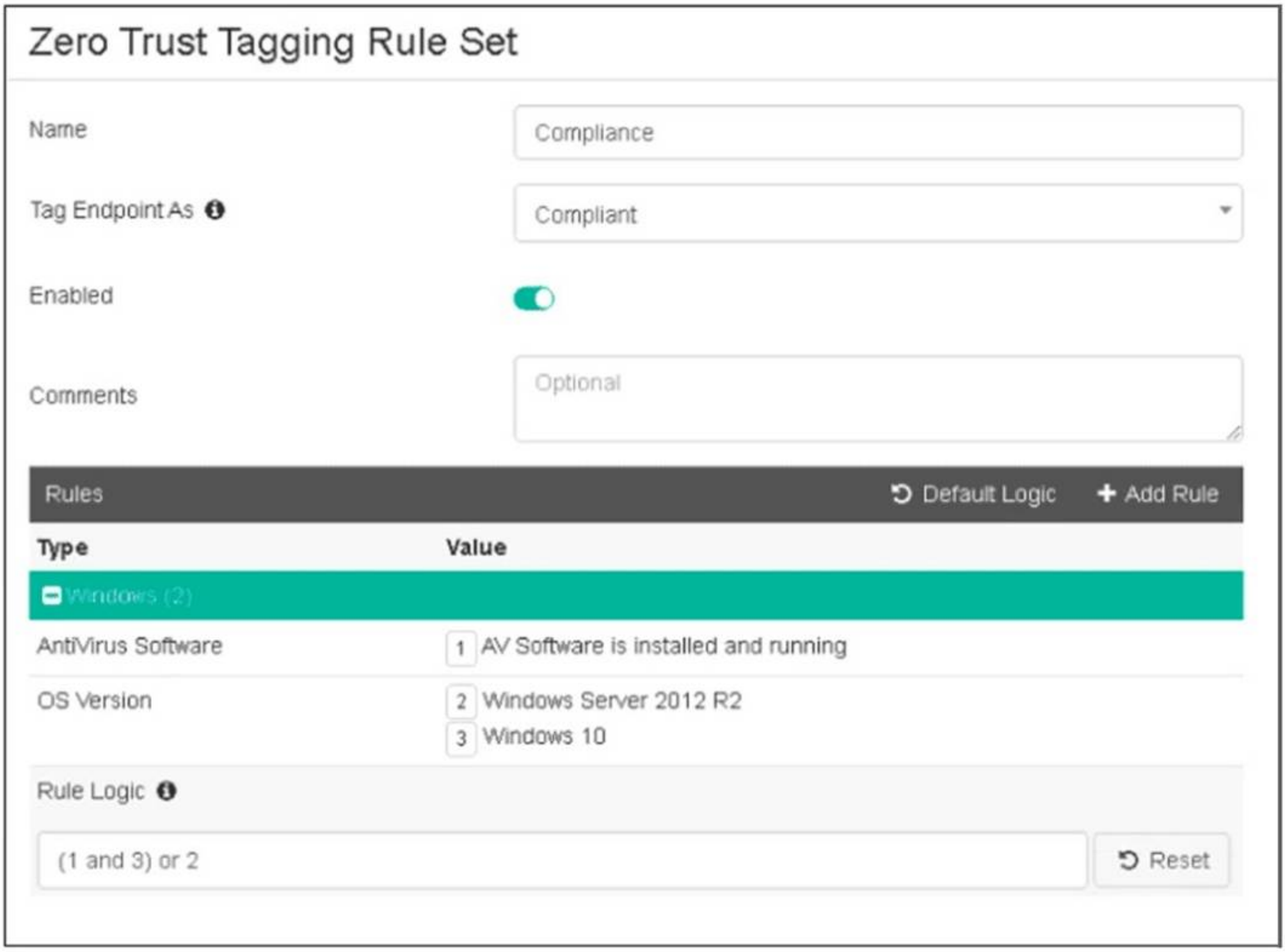


What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

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

NEW QUESTION 25
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 28
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

NEW QUESTION 31
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

NEW QUESTION 32
Which three features does FortiClient endpoint security include? (Choose three.)

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

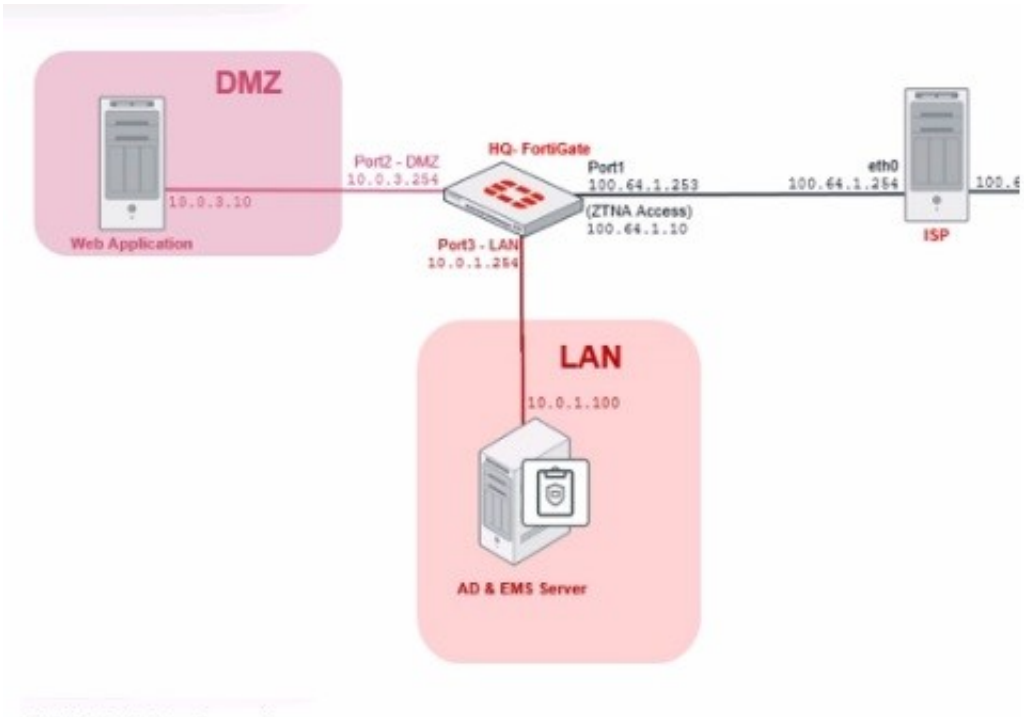
Answer: BDE

NEW QUESTION 35
An administrator installs FortiClient EMS in the enterprise.
Which component is responsible for enforcing protection and checking security posture?

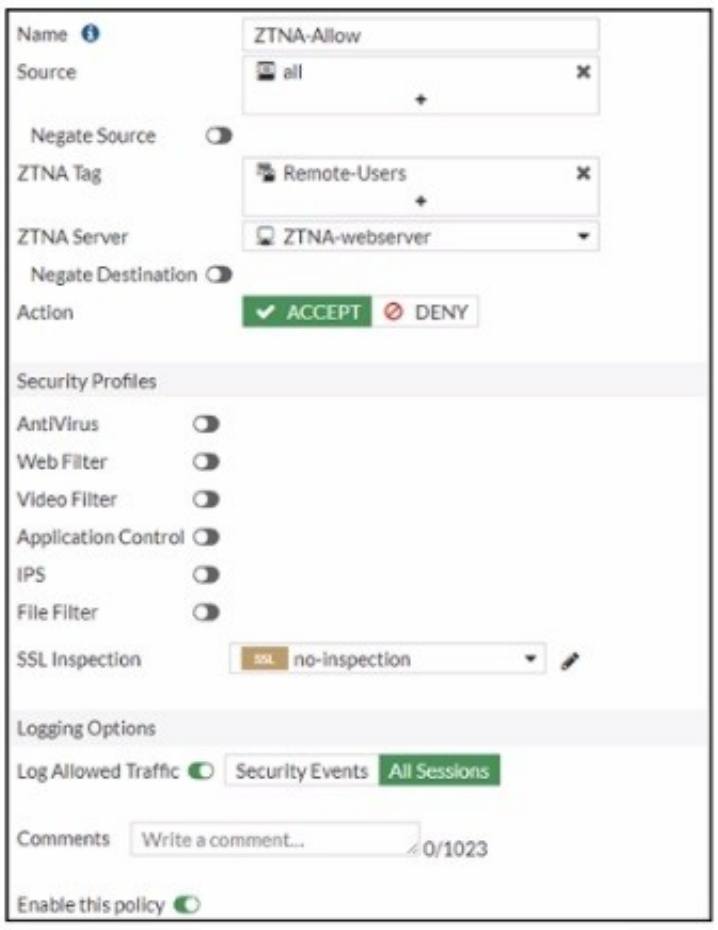
A. FortiClient EMS tags
B. FortiClient vulnerability scan
C. FortiClient
D. FortiClient EMS

Answer: C

NEW QUESTION 38
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.

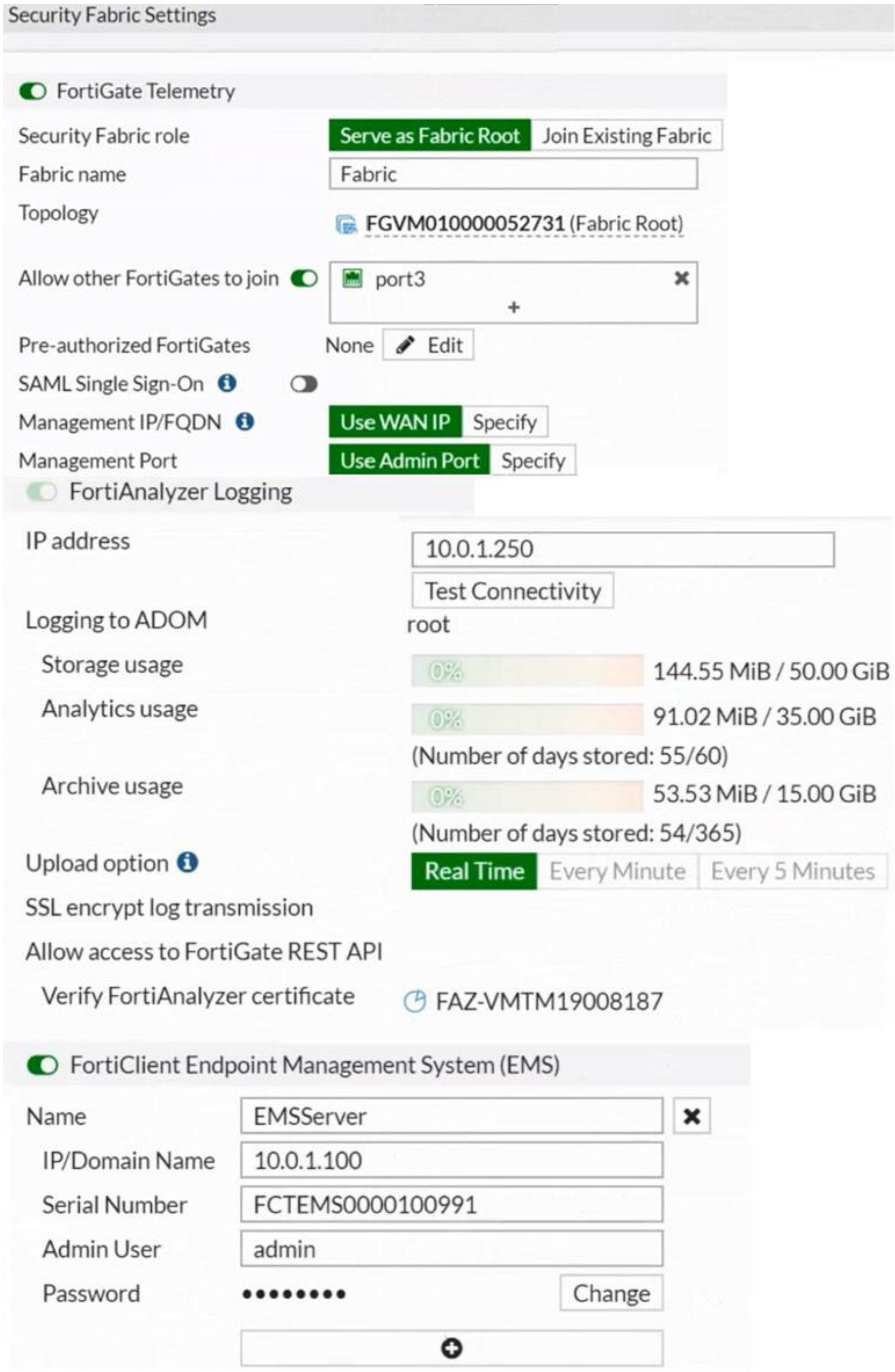
Answer: D

NEW QUESTION 43
Which two statements are true about ZTNA? {Choose two.)

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

Answer: BC

NEW QUESTION 48
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
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.

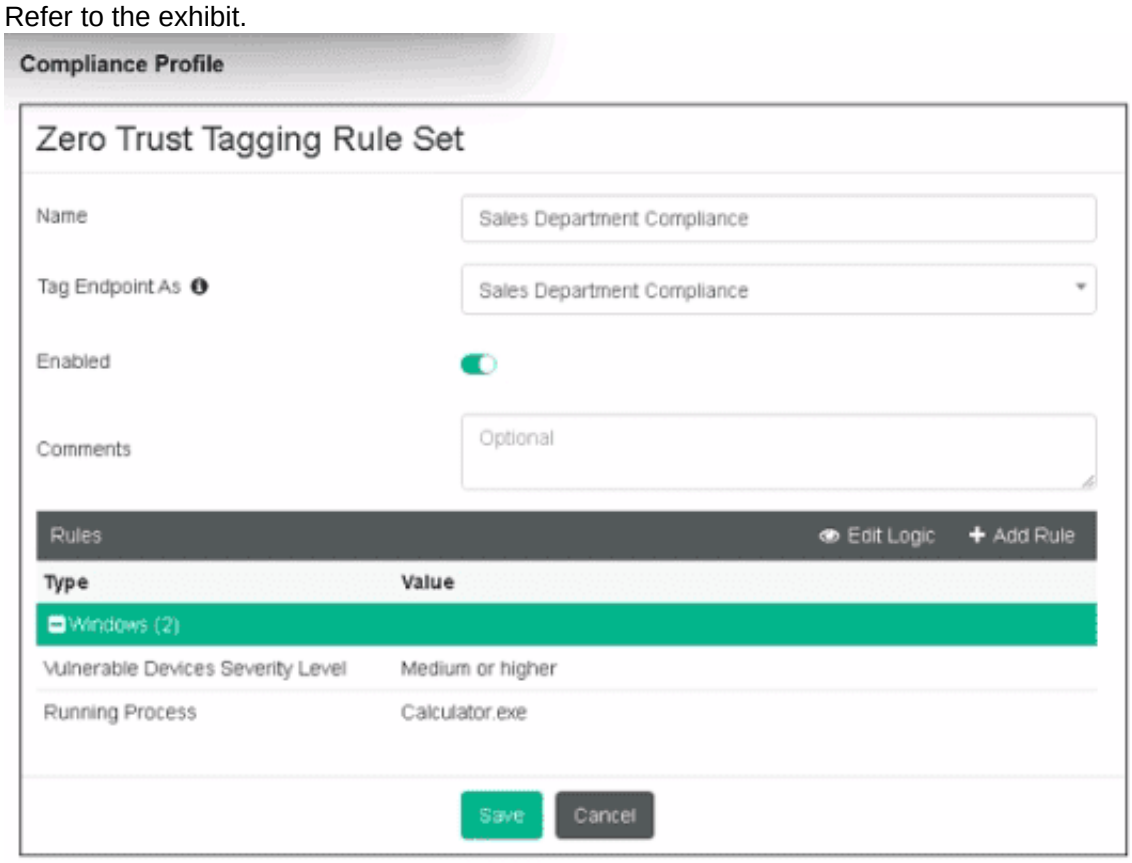
Answer: A

NEW 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

NEW QUESTION 59
Refer to the exhibit.

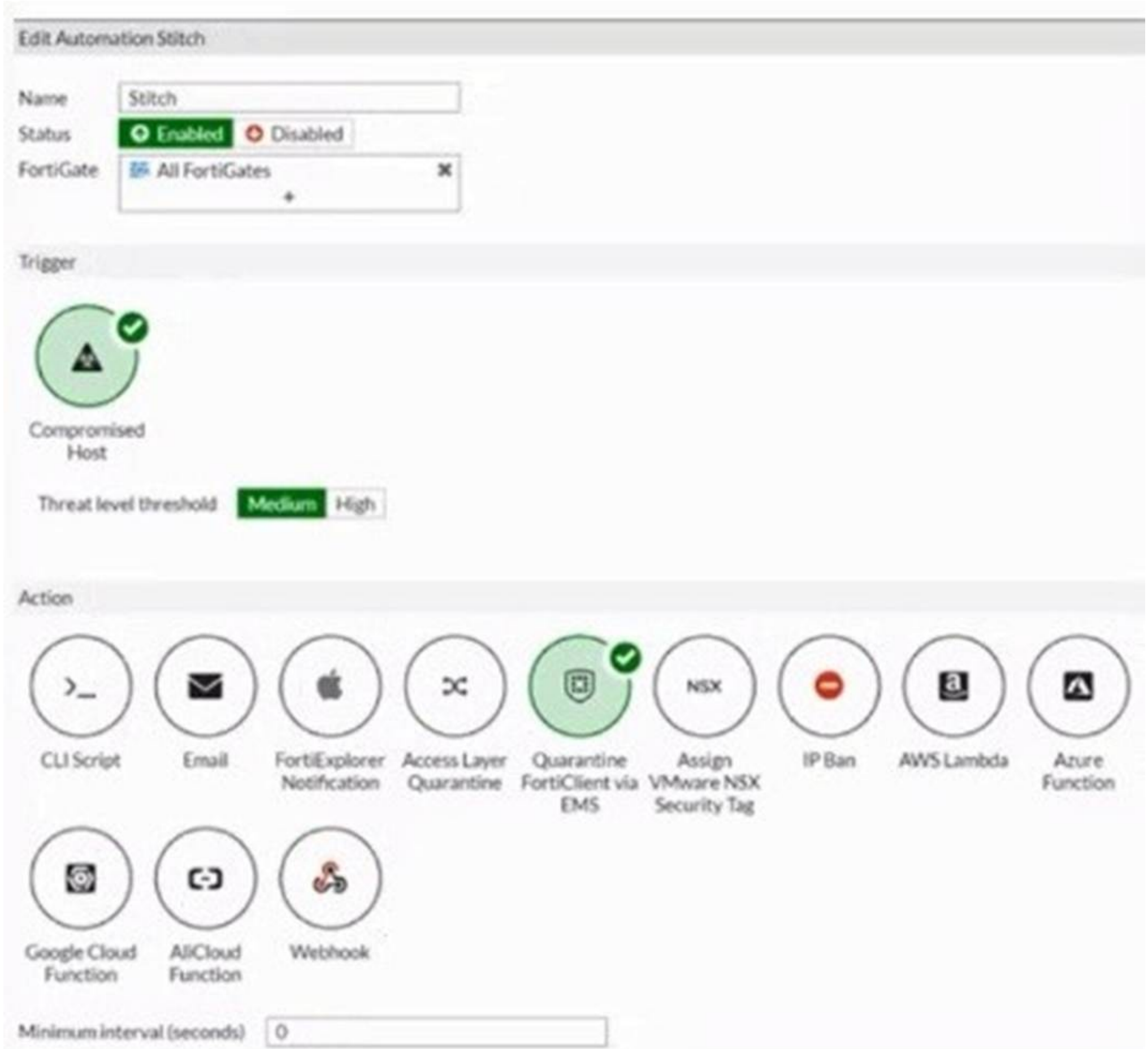


Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

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

NEW QUESTION 61
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 65
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

NEW QUESTION 66
Refer to the exhibit.

FortiClient logs

```
20250226 05:50:24.563 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /
20250226 05:50:24.563 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com
20250226 05:50:24.563 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /
20250226 05:50:24.564 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com / Brave-Dumps.com /
20250226 05:50:24.564 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com / rating: -1 action: WF_ACTION_BLOCK
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 ConnID 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 path /favicon.ico
20250226 05:50:24.821 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /favicon.ico Brave-Dumps.com
20250226 05:50:24.821 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com /favicon.ico rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.821 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com /favicon.ico Unknown 2025-02-26 05:50:24.8212253
+0100 CET m=+4561.294667764 admin 368039 /opt/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

NEW QUESTION 68
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 70
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

NEW QUESTION 74
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FCT_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FCT_AD-7.4-dumps.html