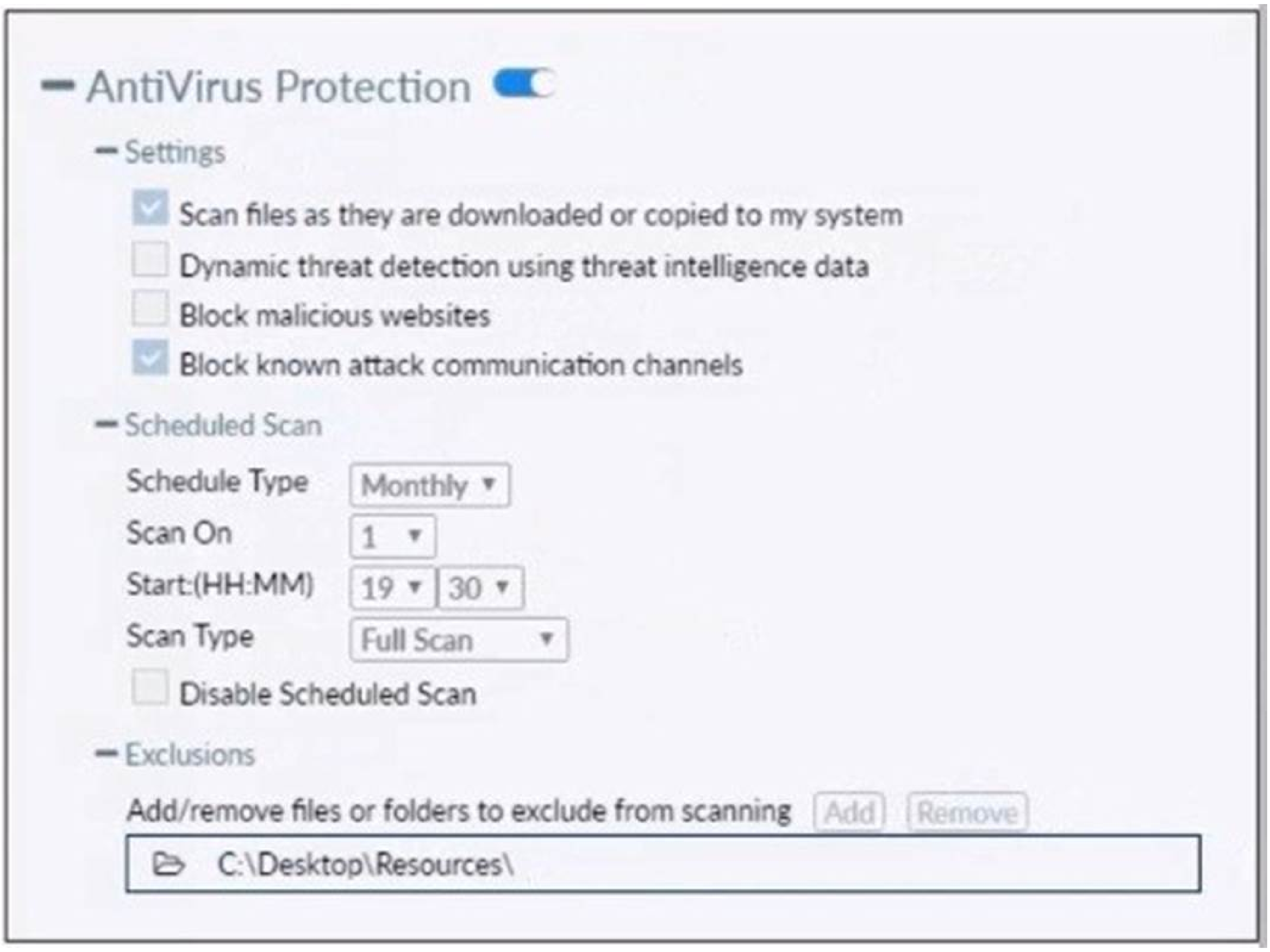
Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

NEW QUESTION 1
Refer to the exhibit.



AntiVirus Protection

Settings

☑ Scan files as they are downloaded or copied to my system
□ Dynamic threat detection using threat intelligence data
□ Block malicious websites
☑ Block known attack communication channels

Scheduled Scan

Schedule Type: Monthly
Scan On: 1
Start:(HH:MM): 19 : 30
Scan Type: Full Scan
□ Disable Scheduled Scan

Exclusions

Add/remove files or folders to exclude from scanning [Add] [Remove]

C:\Desktop\Resources\

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

NEW QUESTION 2
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

Explanation:
? Understanding Quick Scan Function:
? Evaluating Scan Scope:
? Conclusion:
References:
? FortiClient scanning options documentation from the study guides.

NEW QUESTION 3

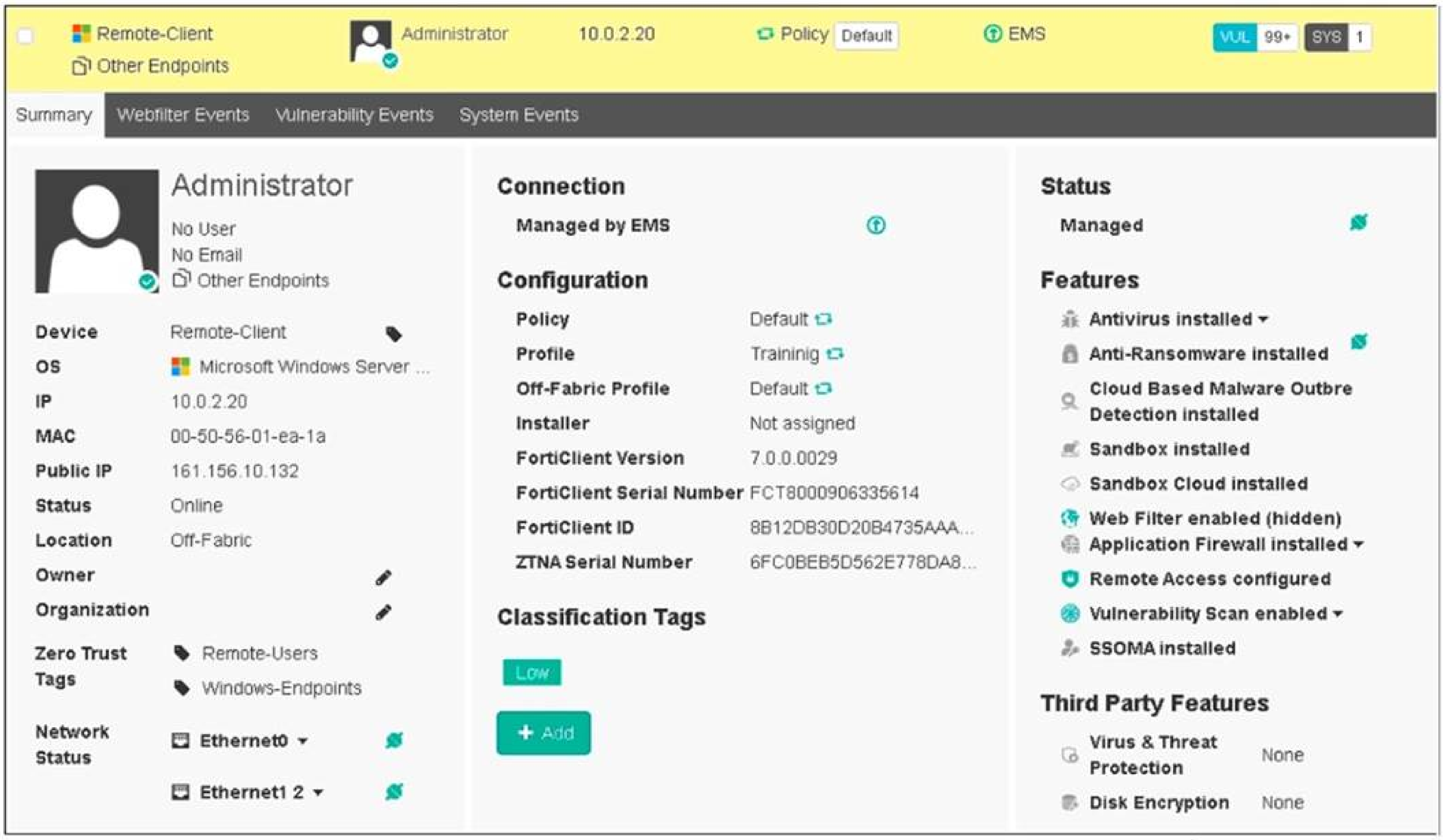
Which two third-party tools can an administrator use to deploy FortiClient? (Choose two.)

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 4
Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.



Remote-Client
Other Endpoints
Administrator
10.0.2.20
Policy Default
EMS
VUL 99+ SYS 1

Administrator
No User
No Email
Other Endpoints

Device	Remote-Client
OS	Microsoft Windows Server ...
IP	10.0.2.20
MAC	00-50-56-01-ea-1a
Public IP	161.156.10.132
Status	Online
Location	Off-Fabric
Owner	
Organization	
Zero Trust Tags	Remote-Users Windows-Endpoints
Network Status	Ethernet0 Ethernet1 2

Connection

Managed by EMS

Configuration

Policy	Default
Profile	Traininig
Off-Fabric Profile	Default
Installer	Not assigned
FortiClient Version	7.0.0.0029
FortiClient Serial Number	FCT8000906335614
FortiClient ID	8B12DB30D20B4735AAA...
ZTNA Serial Number	6FC0BEB5D562E778DA8...

Classification Tags

Low

Status

Managed

Features

- Antivirus installed
- Anti-Ransomware installed
- Cloud Based Malware Outbre Detection installed
- Sandbox installed
- Sandbox Cloud installed
- Web Filter enabled (hidden)
- Application Firewall installed
- Remote Access configured
- Vulnerability Scan enabled
- SSOMA installed

Third Party Features

Virus & Threat Protection	None
Disk Encryption	None

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.
References
? FortiClient EMS 7.2 Study Guide, Endpoint Summary Information Section
? Fortinet Documentation on Endpoint Policies and Status Indicators

NEW QUESTION 5
Which three features does FortiClient endpoint security include? (Choose three.)

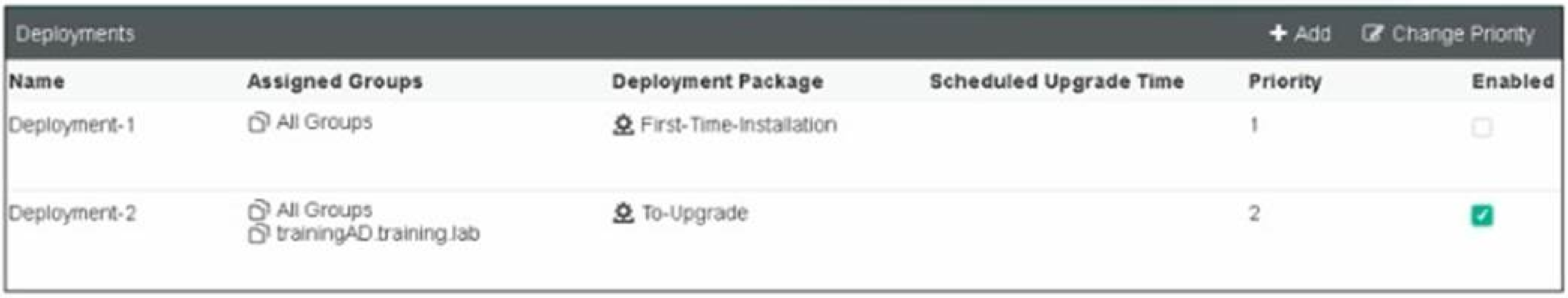
A. DLP
B. Vulnerability management

C. L2TP
D. IPsec
E. Real-lime protection

Answer: BDE

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

NEW QUESTION 6
Refer to the exhibit, which shows FortiClient EMS deployment, profiles.



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

Explanation:
? Deployment Profiles Analysis:
? Evaluating Deployment-2:
? Conclusion:
References:
? FortiClient EMS deployment and profile documentation from the study guides.

NEW QUESTION 7
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 8
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 9
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

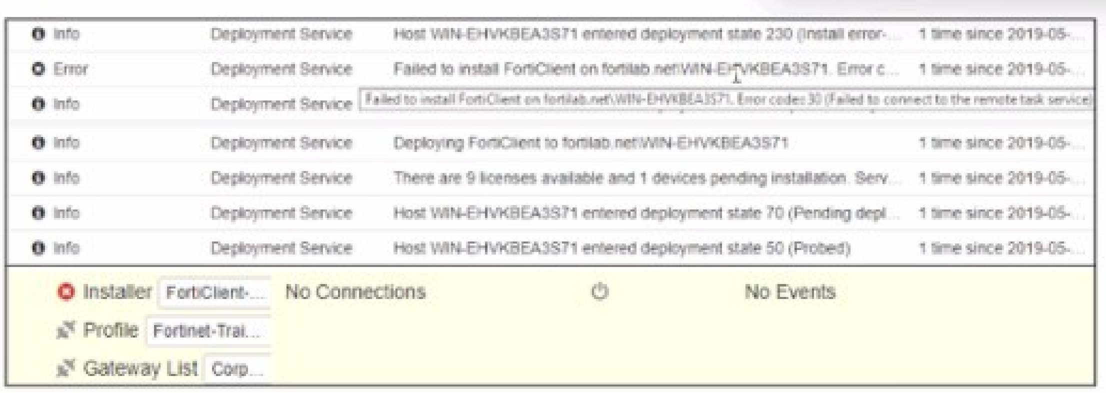
Explanation:
When deploying FortiClient via Microsoft AD Group Policy, it is essential to ensure that the deployment package is correctly assigned to the target group. The absence ofcustom configuration after installation can be due to several reasons, but the most likely cause is:
? Deployment Package 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
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 10
Exhibit.



```
Info    Deployment Service   Host WIN-EHVKBEA3S71 entered deployment state 230 (Install error-...   1 time since 2019-05-...
Error   Deployment Service   Failed to install FortiClient on fortilab.net\WIN-EHVKBEA3S71. Error c...   1 time since 2019-05-...
Info    Deployment Service   Failed to install FortiClient on fortilab.net\WIN-EHVKBEA3S71. Error code: 30 (Failed to connect to the remote task service)
Info    Deployment Service   Deploying FortiClient to fortilab.net\WIN-EHVKBEA3S71   1 time since 2019-05-...
Info    Deployment Service   There are 9 licenses available and 1 devices pending installation. Serv...   1 time since 2019-05-...
Info    Deployment Service   Host WIN-EHVKBEA3S71 entered deployment state 70 (Pending depl...   1 time since 2019-05-...
Info    Deployment Service   Host WIN-EHVKBEA3S71 entered deployment state 50 (Probed)   1 time since 2019-05-...

Installer    FortiClient-...   No Connections        No Events
Profile      Fortinet-Trai...
Gateway List Corp...
```

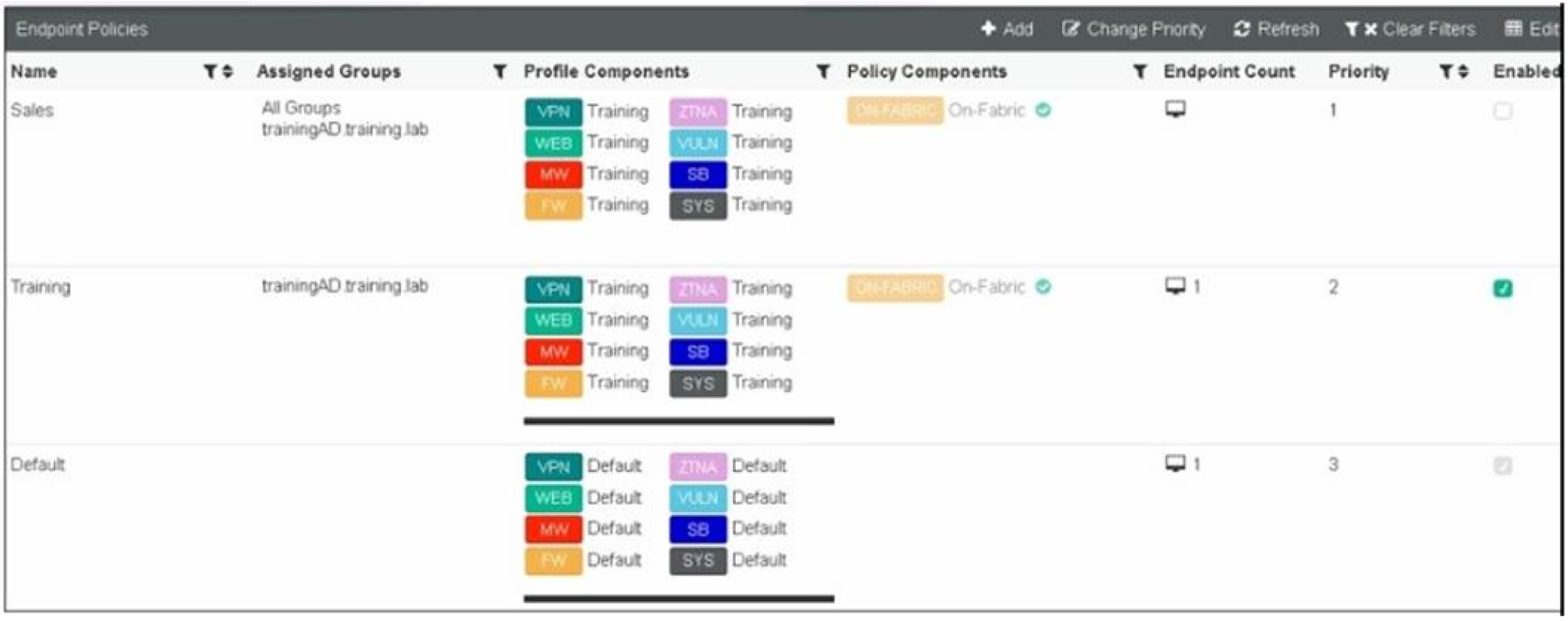
Based on the logs shown in the exhibit, why did FortiClient EMS tail to install FortiClient on the endpoint?

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 13
FortiClient EMS endpoint policies



Endpoint Policies

Name	Assigned Groups	Profile Components	Policy Components	Endpoint Count	Priority	Enabled
Sales	All Groups trainingAD.training.lab	VPN Training WEB Training MW Training FW Training ZTNA Training VULN Training SB Training SYS Training	ON-FABRIC On-Fabric ✓		1	☐
Training	trainingAD.training.lab	VPN Training WEB Training MW Training FW Training ZTNA Training VULN Training SB Training SYS Training	ON-FABRIC On-Fabric ✓	1	2	☑
Default		VPN Default WEB Default MW Default FW Default ZTNA Default VULN Default SB Default SYS Default		1	3	☑

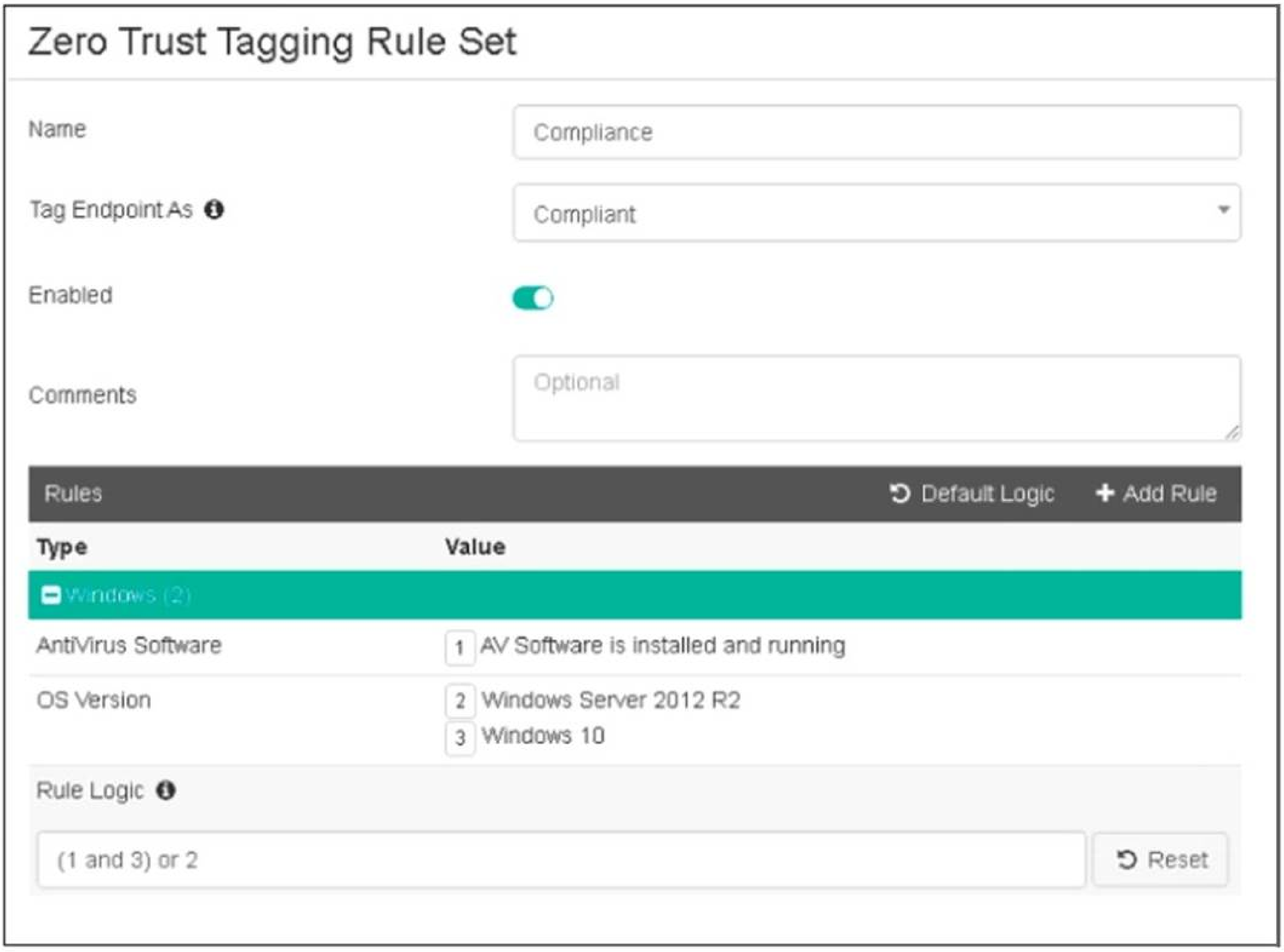
Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

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:
? Evaluating Policy Assignment:
? Conclusion:
References:
? FortiClient EMS policy configuration and priority management documentation from the study guides.

NEW QUESTION 16
Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.



Zero Trust Tagging Rule Set

Name: Compliance

Tag Endpoint As: Compliant

Enabled

Comments: Optional

Type	Value
Windows (2)	
AntiVirus Software	1 AV Software is installed and running
OS Version	2 Windows Server 2012 R2 3 Windows 10

Rule Logic: (1 and 3) or 2

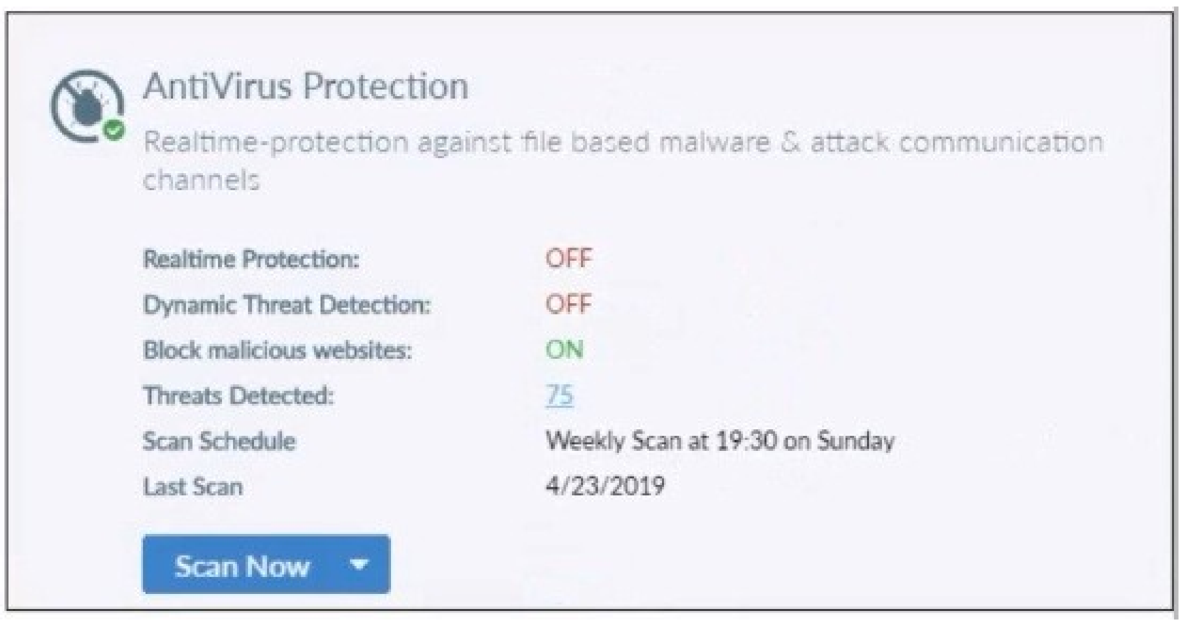
Which two statements about the rule set are true? (Choose two.)

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:
? The Rule Logic is specified as "(1 and 3) or 2," meaning: Therefore, the endpoint must satisfy either:
? Antivirus is installed and running and Windows 10 is running.
? Windows Server 2012 R2 is running.
References
? FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Rule Set Configuration Section
? Fortinet Documentation on Configuring Zero Trust Tagging Rules and Logic

NEW QUESTION 17
Refer to the exhibit.



AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Realtime Protection: OFF
Dynamic Threat Detection: OFF
Block malicious websites: ON
Threats Detected: 75
Scan Schedule Weekly Scan at 19:30 on Sunday
Last Scan 4/23/2019

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.
References
? FortiClient EMS 7.2 Study Guide, Antivirus Protection Section
? Fortinet Documentation on FortiClient Real-time Protection Settings

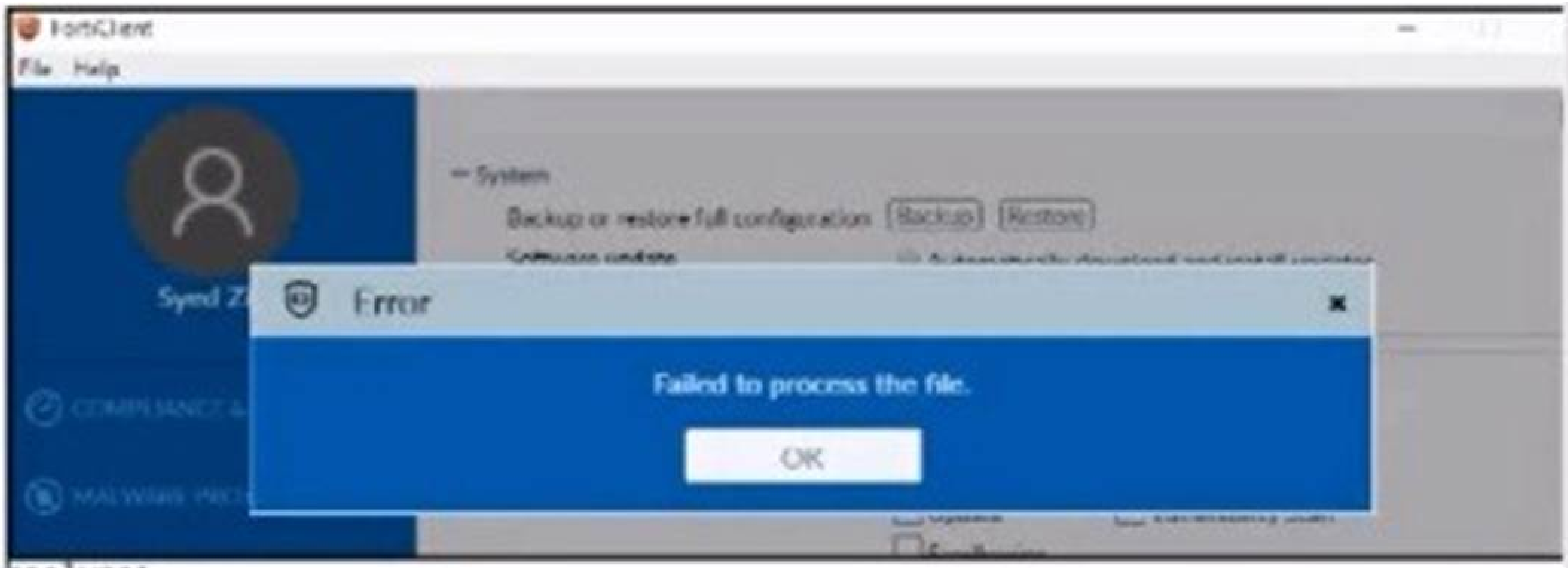
NEW QUESTION 18
Which statement about FortiClient comprehensive endpoint protection is true?

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.

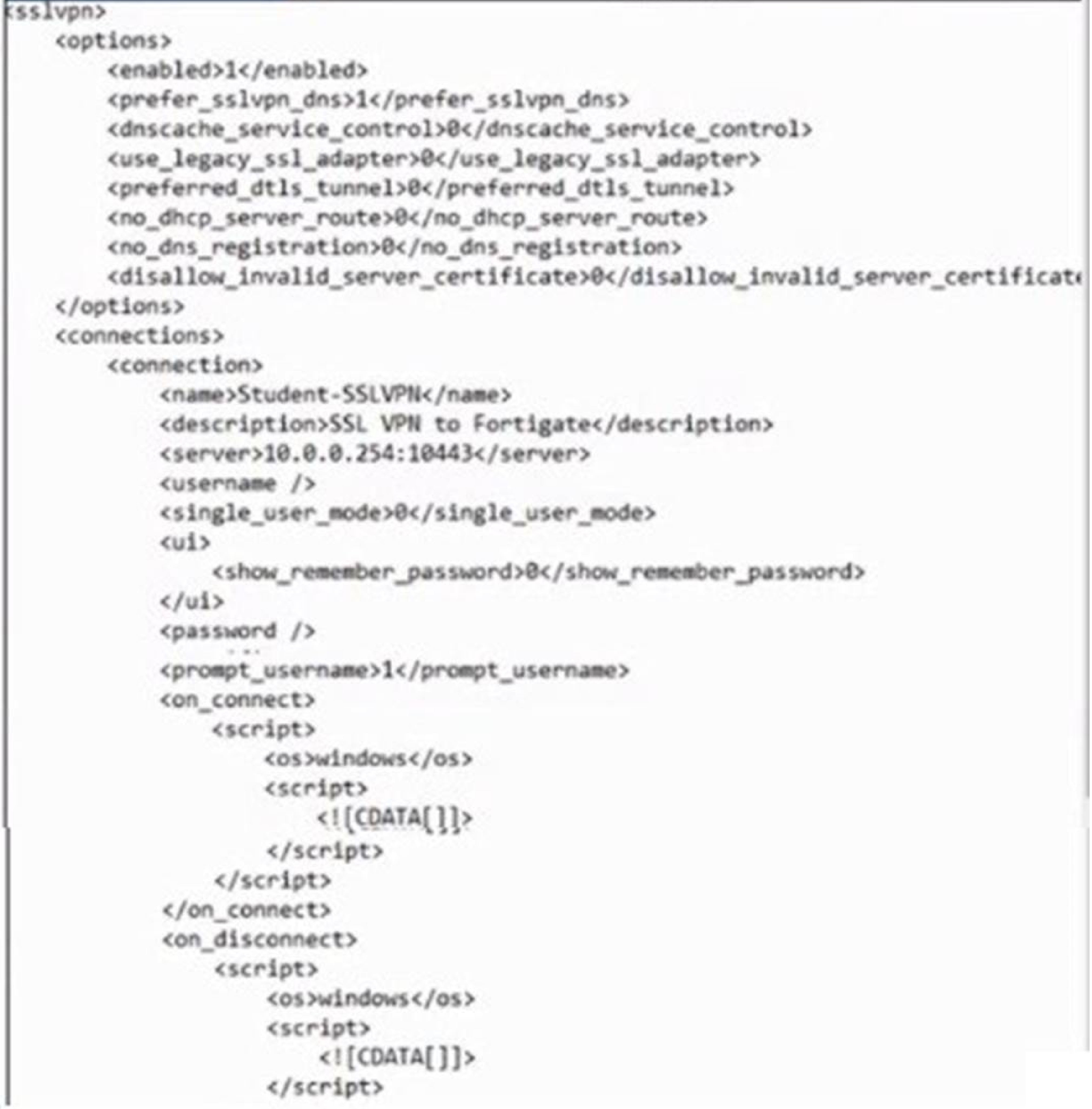
Answer: D

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.

NEW QUESTION 21
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

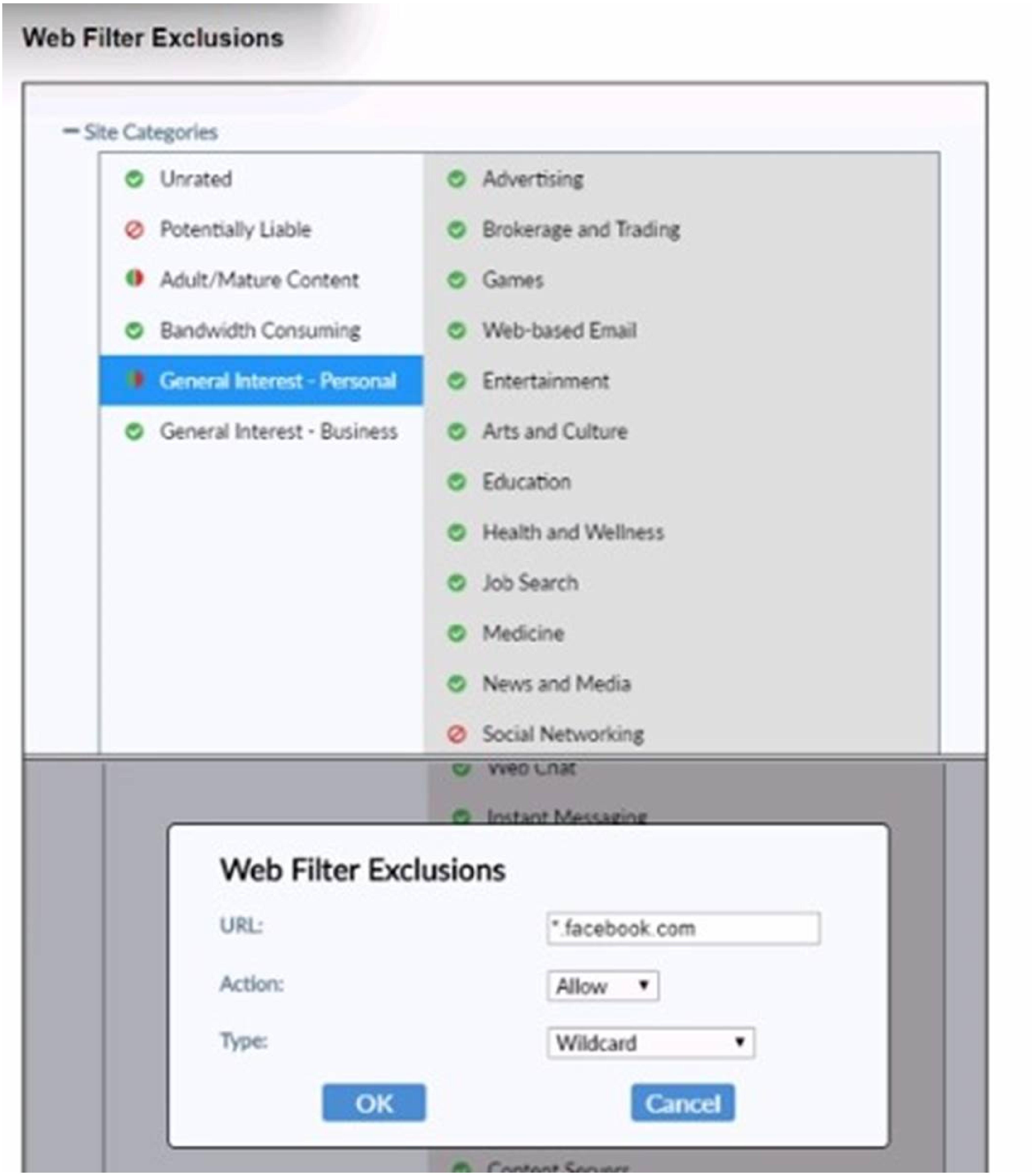
NEW QUESTION 23
Which security fabric component sends a notification io quarantine an endpoint after IOC detection "n the automation process?

A. FortiAnalyzer
B. FortiGate
C. FortiClient EMS
D. FortiClient

Answer: C

Explanation:
? Understanding the Automation Process:
? Evaluating Responsibilities:
? Conclusion:
References:
? FortiClient EMS and automation process documentation from the study guides.

NEW QUESTION 26
Refer to the exhibit.



Web Filter Exclusions

− Site Categories

✓ Unrated	✓ Advertising
⊘ Potentially Liable	✓ Brokerage and Trading
◐ Adult/Mature Content	✓ Games
✓ Bandwidth Consuming	✓ Web-based Email
◐ General Interest - Personal	✓ Entertainment
✓ General Interest - Business	✓ Arts and Culture
	✓ Education
	✓ Health and Wellness
	✓ Job Search
	✓ Medicine
	✓ News and Media
	⊘ Social Networking
	✓ Web Chat
	✓ Instant Messaging
	✓ Content Servers

Web Filter Exclusions

URL: *.facebook.com

Action: Allow

Type: Wildcard

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:
? Evaluating Actions:
? Conclusion:
References:
? FortiClient web filter configuration and exclusion documentation from the study guides.

NEW QUESTION 30

......