Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 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
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

Explanation:
? Understanding the Need for Root CA Certificate:
? Evaluating Use Cases:
? Conclusion:
References:
? FortiClient EMS and FortiGate certificate management documentation from the study guides.

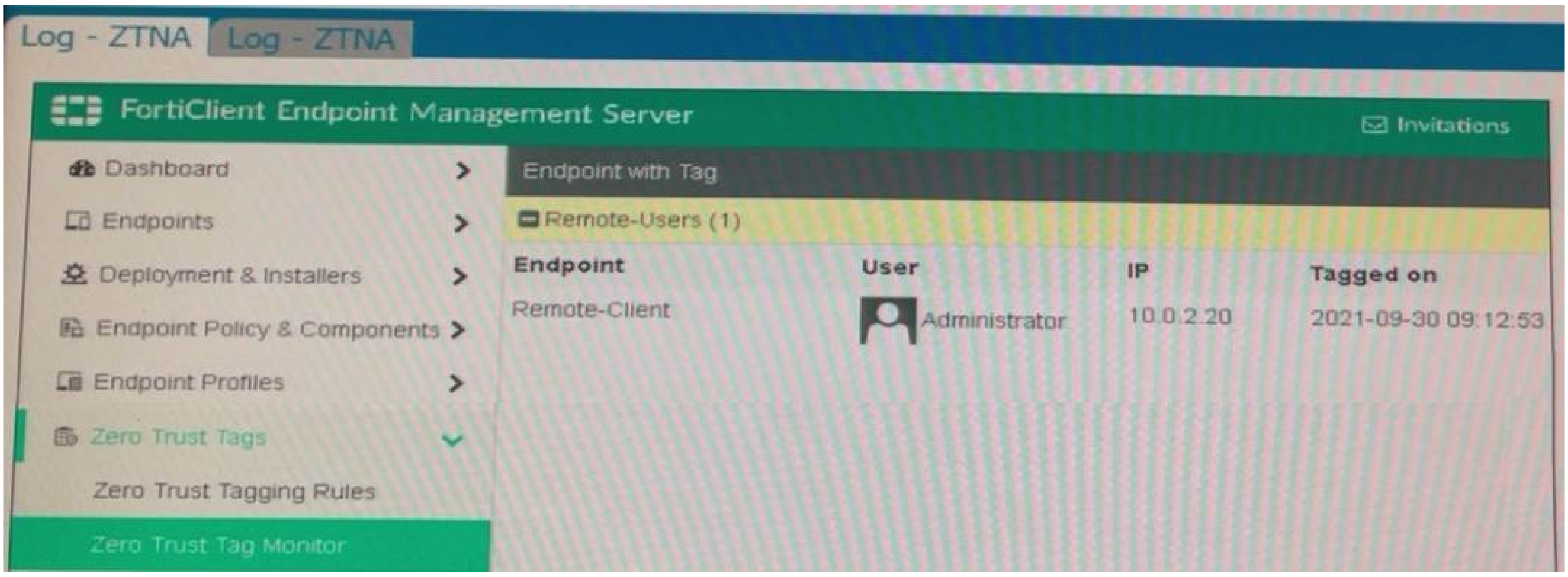
NEW QUESTION 5
Which two statements are true about ZTNA? {Choose two.)

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

Explanation:
ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.
Two functions of ZTNA are:
ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the
device's software and hardware configurations, security settings, and the presence of malware.
ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

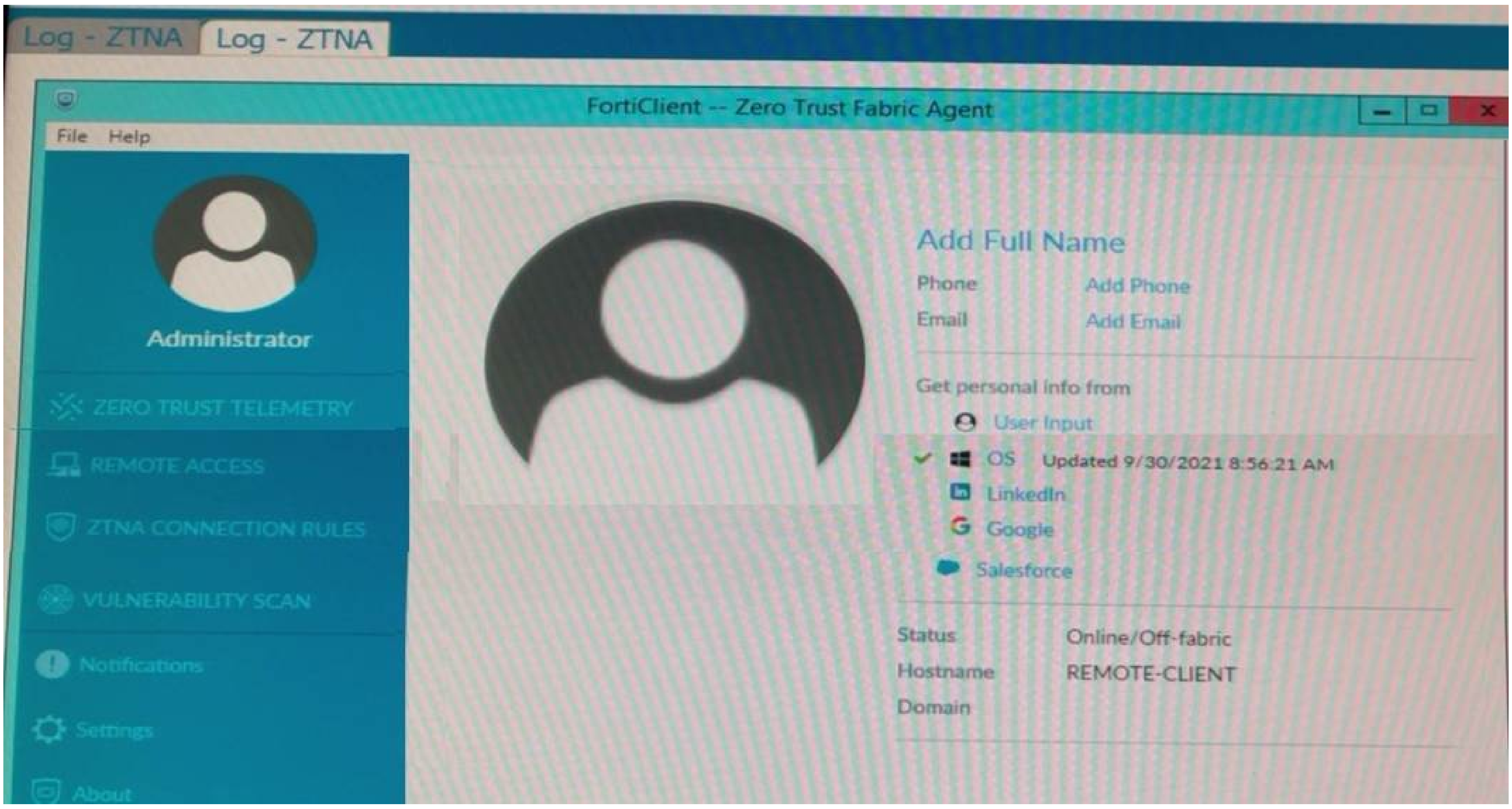
NEW QUESTION 6
Refer to the exhibits.



Endpoint with Tag

Remote-Users (1)

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



Phone Add Phone
Email Add Email

✓ OS Updated 9/30/2021 8:56:21 AM

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

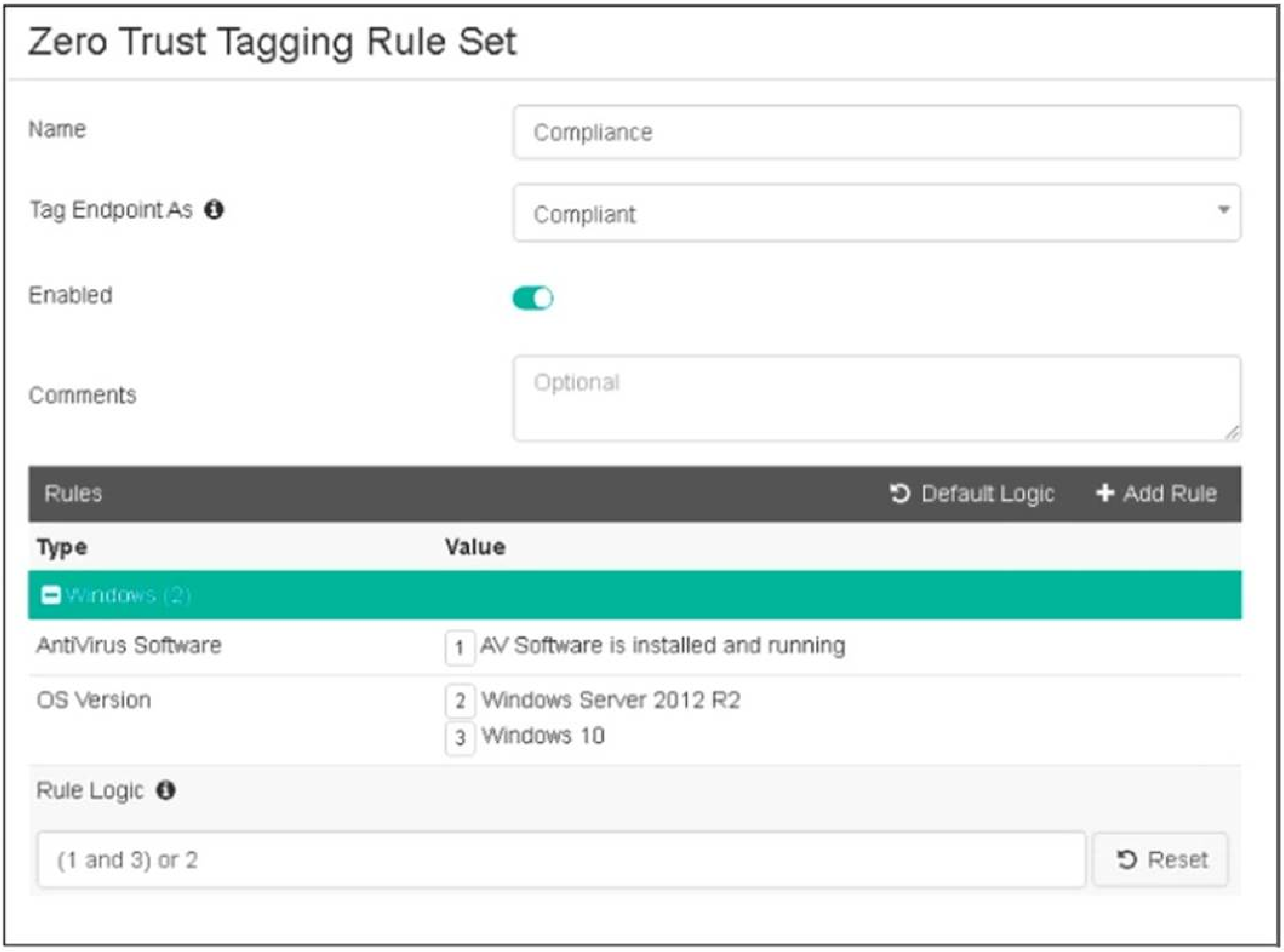
NEW QUESTION 7
An administrator installs FortiClient on Windows Server. What is the default behavior of real-time protection control?

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

Explanation:
When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:
? Real-time protection is disabled:By default, FortiClient does not enable real-time
protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints.
Thus, real-time protection is disabled by default on Windows Server installations.
References
? FortiClient EMS 7.2 Study Guide, Real-time Protection Section
? Fortinet Documentation on FortiClient Default Settings for Server Installations

NEW QUESTION 8
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

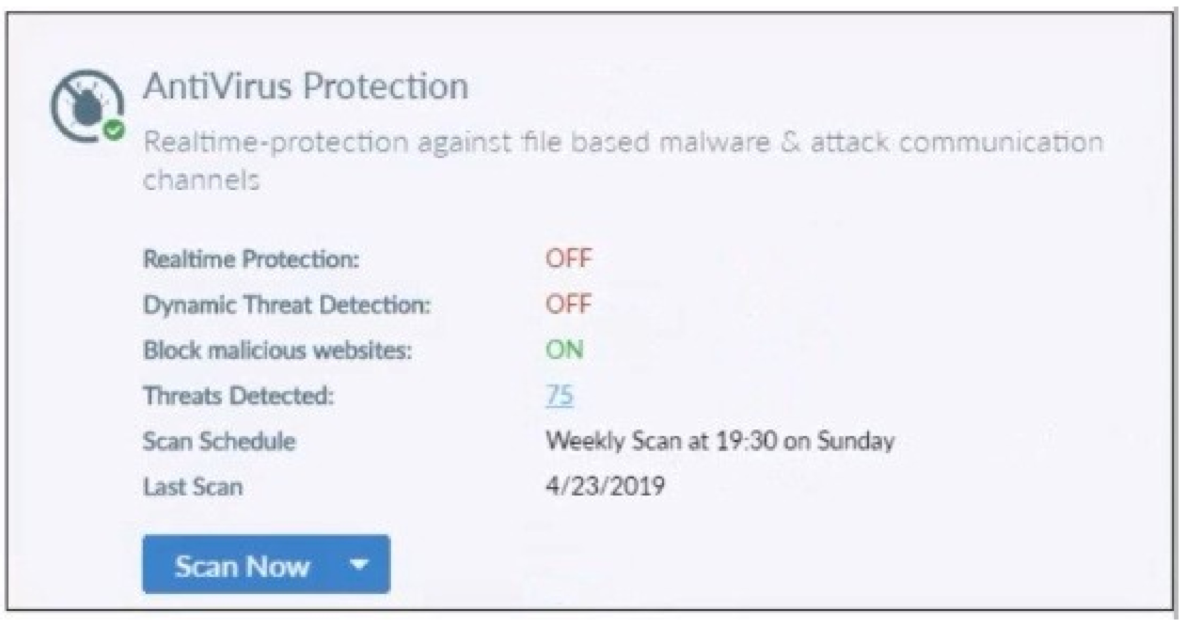
Which two statements about the rule set are true? (Choose two.)

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 9
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

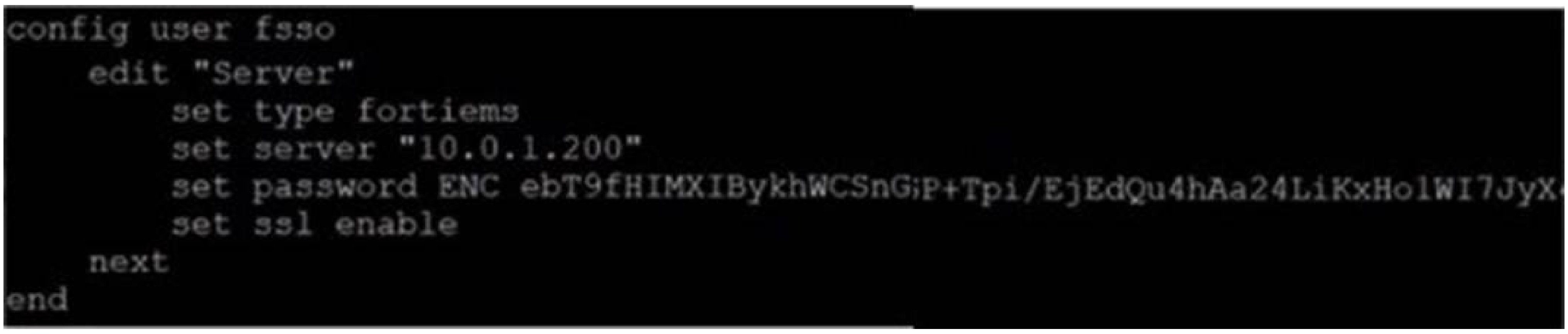
Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

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 10
Refer to the exhibit.



```
config user fsso
    edit "Server"
        set type fortiems
        set server "10.0.1.200"
        set password ENC ebT9fHIMXIBykhWCSnGiP+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 10
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 12
......

Relate Links

100% Pass Your FCP_FCT_AD-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FCT_AD-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/