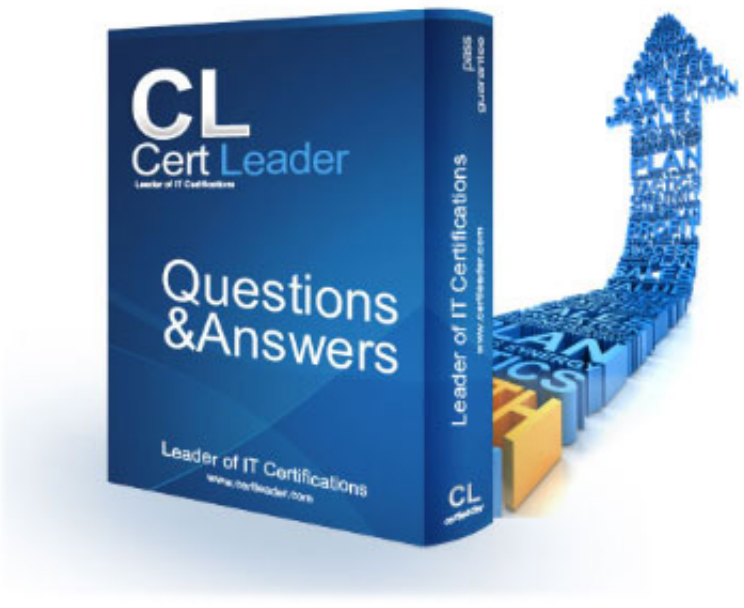
FCP_FCT_AD-7.2 Dumps

FCP-FortiClient EMS 7.2 Administrator

https://www.certleader.com/FCP_FCT_AD-7.2-dumps.html



NEW QUESTION 1
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 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.

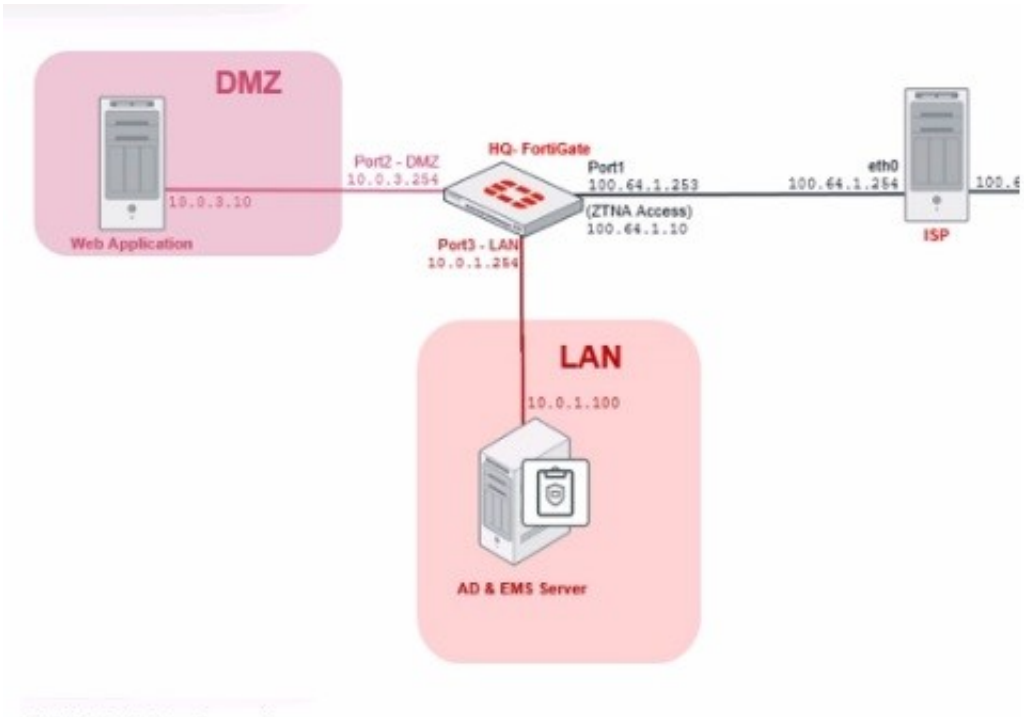
NEW QUESTION 3
Which two statements are true about the ZTNA rule? (Choose two.)

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.

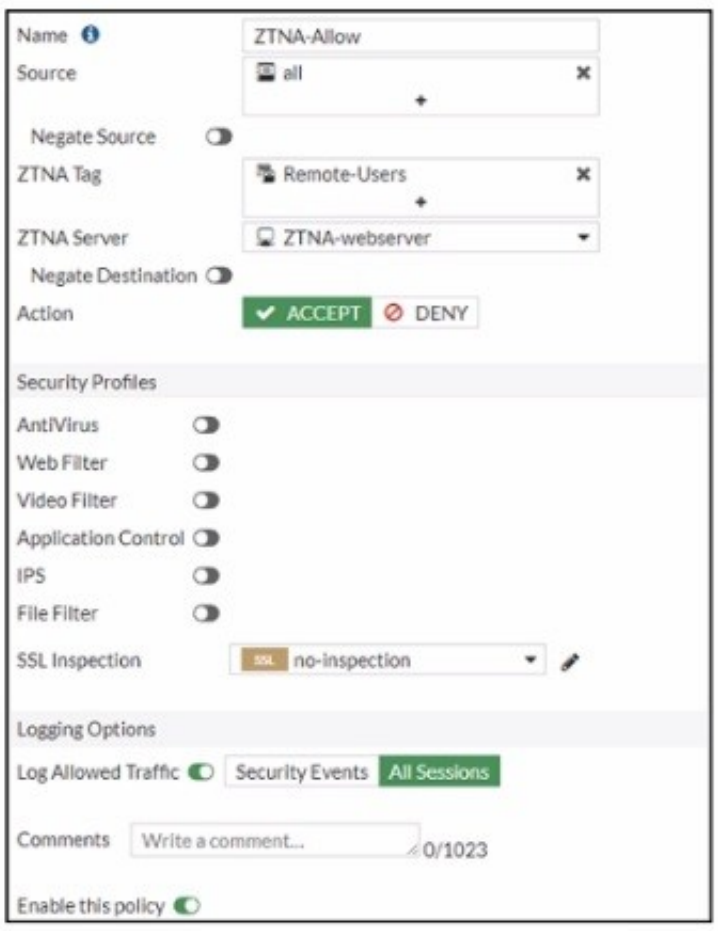
Answer: AD

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

NEW QUESTION 4
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 5
Refer to the exhibit.

Based on The settings shown in The exhibit, which statement about FortiClient behaviour is Hue?

A. FortiClient scans infected files when the user copies files to the Resources folder.
B. FortiClient quarantines infected ties and reviews later, after scanning them.
C. FortiClient copies infected files to the Resources folder without scanning them.
D. FortiClient blocks and deletes infected files after scanning them.

Answer: A

Explanation:
Based on the settings shown in the exhibit, FortiClient is configured to scan files as they are downloaded or copied to the system. This means that if a user copies files to the ??Resources?? folder, which is not listed under exclusions, FortiClient will scan these files for infections. The exclusion path mentioned in the settings, "C:\Users\Administrator\Desktop\Resources", indicates that any files copied to this specific folder will not be scanned, but since the question implies that the ??Resources?? folder is not the same as the excluded path, FortiClient will indeed scan the files for infections.

NEW QUESTION 6
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

Explanation:
? Understanding ZTNA:
? Evaluating Components:
? Conclusion:
References:
? ZTNA and FortiClient EMS configuration documentation from the study guides.

NEW QUESTION 7

Which statement about FortiClient enterprise management server is true?

A. It provides centralized management of FortiGate devices.
B. lt provides centralized management of multiple endpoints running FortiClient software.
C. It provides centralized management of FortiClient Android endpoints only.
D. It provides centralized management of Chromebooks running real-time protection

Answer: B

Explanation:
FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

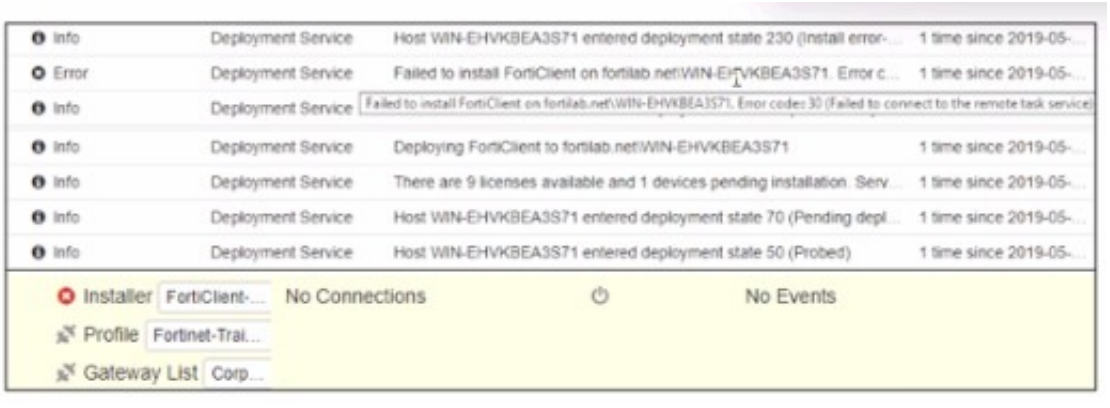
NEW QUESTION 8
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing. What could have caused this problem?

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 9
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

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 10
Which component or device shares ZTNA tag information through Security Fabric integration?

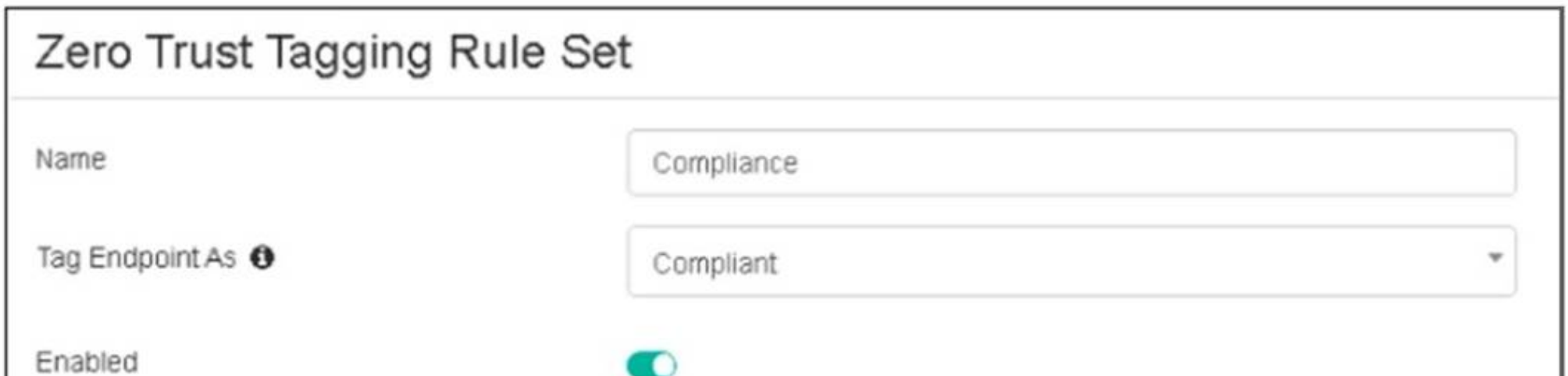
A. FortiGate
B. FortiGate Access Proxy
C. FortiClient

Answer: A

Explanation:
FortiClient EMS is the component that shares ZTNA tag information through Security Fabric integration. ZTNA tags are synchronized from FortiClient EMS as inputs for the FortiGate application gateway. They can be used in ZTNA policies as security posture checks to ensure certain security criteria are met. FortiClient EMS can share ZTNA tags across multiple devices in the Fabric, such as FortiGate, FortiManager, and FortiAnalyzer. FortiClient EMS can also share ZTNA tags across multiple VDOMs on thesame FortiGate device. FortiClient EMS can be configured to control the ZTNA tag sharing behavior in the Fabric Devices settings1.

FortiGate is the device that enforces ZTNA policies using ZTNA tags. FortiGate can receive ZTNA tags from FortiClient EMS via Fabric Connector. FortiGate can also publish ZTNA services through the ZTNA portal, which allows users to access applications without installing FortiClient. FortiGate can also provide ZTNA inline CASB for SaaS application access control2.
FortiGate Access Proxy is a feature that enables FortiGate to act as a proxy for ZTNA traffic. FortiGate Access Proxy can be deployed in front of the application servers to provide ZTNA protection. FortiGate Access Proxy can also be deployed behind the application servers to provide ZTNA visibility. FortiGate Access Proxy can use ZTNA tags to identify and authenticate users and devices2.
FortiClient is the endpoint software that connects to ZTNA services. FortiClient can register ZTNA tags with FortiClient EMS based on the endpoint security posture. FortiClient can also use ZTNA tags to access ZTNA services published by FortiGate. FortiClient can also use ZTNA tags to access SaaS applications with ZTNA inline CASB2.
References :=
? Technical Tip: Behavior of ZTNA Tags shared across multiple vdoms or multiple FortiGate firewalls in the Security Fabric connected to the same FortiClient EMS Server
? Synchronizing FortiClient ZTNA tags
? Zero Trust Network Access (ZTNA) to Control Application Access

NEW QUESTION 10
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

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 13
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

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

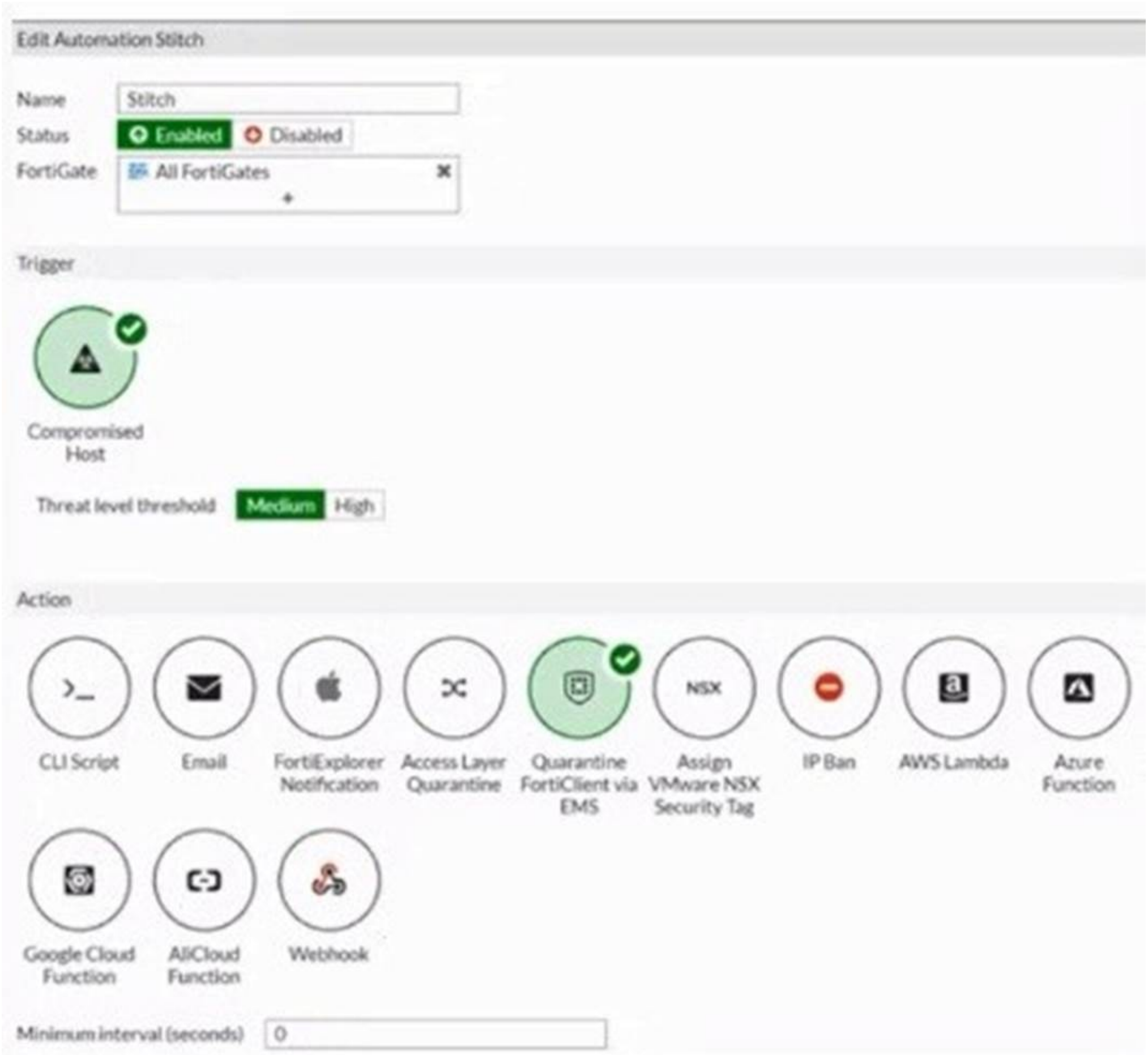
NEW QUESTION 18
Which three types of antivirus scans are available on FortiClient? (Choose three)

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 19
Refer to the exhibit.



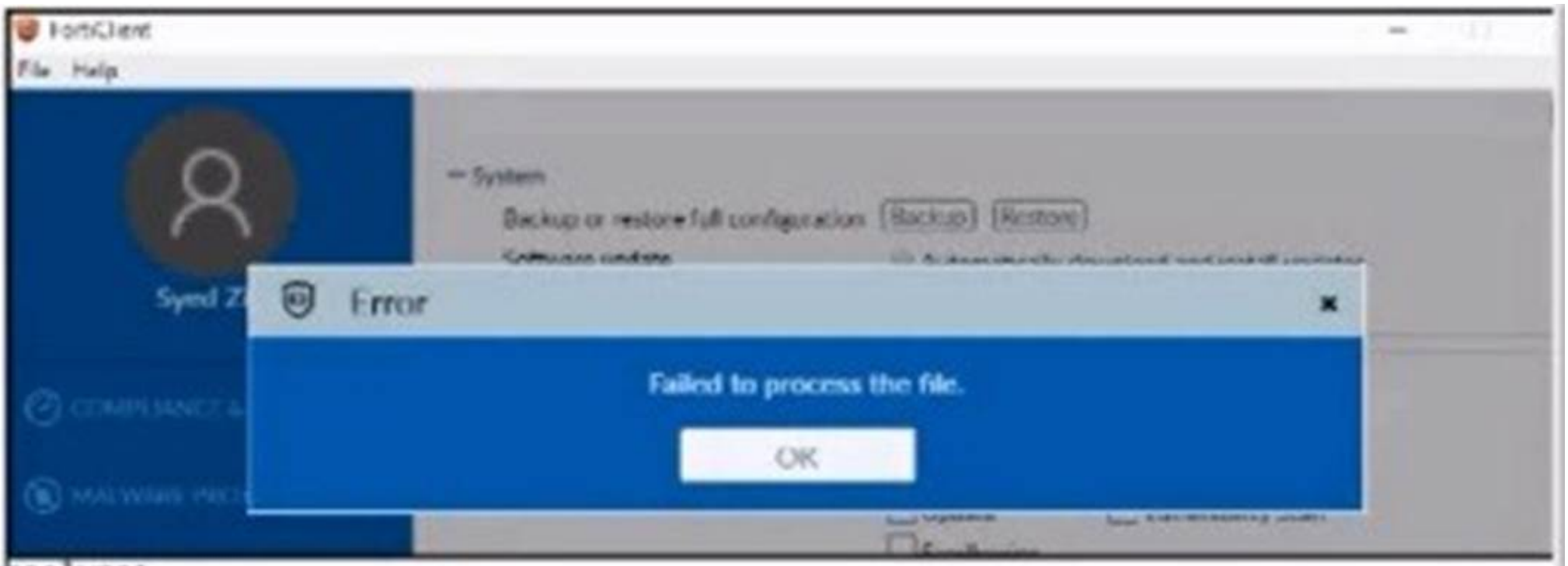
Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

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

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 20
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

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
.....

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-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FCT_AD-7.2-dumps.html