

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

Which statement about the FortiClient enterprise management server is true?

- A. It receives the configuration information of endpoints from FortiGate.
- 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 certificates.

Answer: C

NEW QUESTION 3

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 threats.
- 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 4

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 5

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 6

Why does FortiGate need the root CA certificate of FortiClient 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 7

An administrator has a requirement to add user authentication to the ZTNA access for remote or off-fabric users Which FortiGate feature is required in addition to ZTNA?

A. FortiGate FSSO

B. FortiGate certificates

C. FortiGate explicit proxy

D. FortiGate endpoint control

Answer: C

Explanation:

For adding user authentication to the ZTNA access for remote or off-fabric users, the following FortiGate feature is required in addition to ZTNA:

? FortiGate explicit proxy allows FortiGate to intercept web traffic for authentication purposes.
? ZTNA integrates with various FortiGate features to provide secure access and ensure that users are authenticated before accessing resources.
? By using an explicit proxy, FortiGate can handle web traffic and enforce authentication policies for remote users who are not directly on the corporate network (off-fabric).
Thus, the correct feature to use for this requirement is the FortiGate explicit proxy.
References
? FortiGate Security 7.2 Study Guide, ZTNA and Proxy Configuration Sections
? Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW QUESTION 8

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

Explanation:

Based on the FortiClient logs shown in the exhibit:

? The first log entry shows the application "firefox.exe" trying to access a destination IP, with the threat identified as "Twitter."

? The action taken by the application firewall is "blocked" with the event type "appfirewall."

This indicates that the application firewall has blocked access to Twitter.

References

? FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section

? Fortinet Documentation on Interpreting FortiClient Logs

NEW QUESTION 9

Refer to the exhibit.

AV Protection Settings

— AntiVirus Protection 

— Settings

☒ Scan files as they are downloaded or copied to my system

☐ Antimalware Scan Interface (AMSI)

☐ Dynamic threat detection using threat intelligence data

— Scheduled Scan

Schedule Type

Scan On

Start:(HH:MM)

Scan Type

☐ Disable Scheduled Scan

— Exclusions

Add/remove files or folders to exclude from scanning

 C:\Users\Administrator\Desktop\Resources\

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 files 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 10

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 10

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	<input type="checkbox"/>		
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade		2	<input checked="" type="checkbox"/>		

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 13

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

Explanation:

- ? Understanding FortiClient EMS Components:
 - ? Evaluating Responsibilities:
 - ? Conclusion:
- References:
- ? FortiClient EMS and endpoint security documentation from the study guides.

NEW QUESTION 18

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" countstna=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

Explanation:

- ? Observation of ZTNA Traffic Log:
 - ? Evaluating Log Message:
 - ? Conclusion:
- References:
- ? ZTNA traffic log analysis and configuration documentation from the study guides.

NEW QUESTION 22

Which statement about FortiClient enterprise management server is true?

- A. It provides centralized management of FortiGate devices.
- B. It 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 27

Which component or device shares device status information through ZTNA telemetry?

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

Answer: A

Explanation:

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

NEW QUESTION 28

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 of custom 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 32

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

Explanation:

? Understanding Compliance Rules:

? Enforcing Compliance:

? Conclusion:

References:

? Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

NEW QUESTION 37

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

Explanation:

? Requirement:

? Solution Analysis:

? Evaluating Options:

? Conclusion:

References:

? FortiClient EMS and FortiGate configuration and deployment documentation from the study guides.

NEW QUESTION 41

FortiClient EMS endpoint policies

Endpoint Policies									
+ Add Change Priority Refresh Clear Filters Edit									
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	ON-FABRIC On-Fabric	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 42

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

Explanation:

FortiClient supports initiating the following VPN types from the Windows command prompt:

? IPSec VPN:FortiClient can establish IPSec VPN connections using command line instructions.

? SSL VPN:FortiClient also supports initiating SSL VPN connections from the Windows command prompt.

These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.

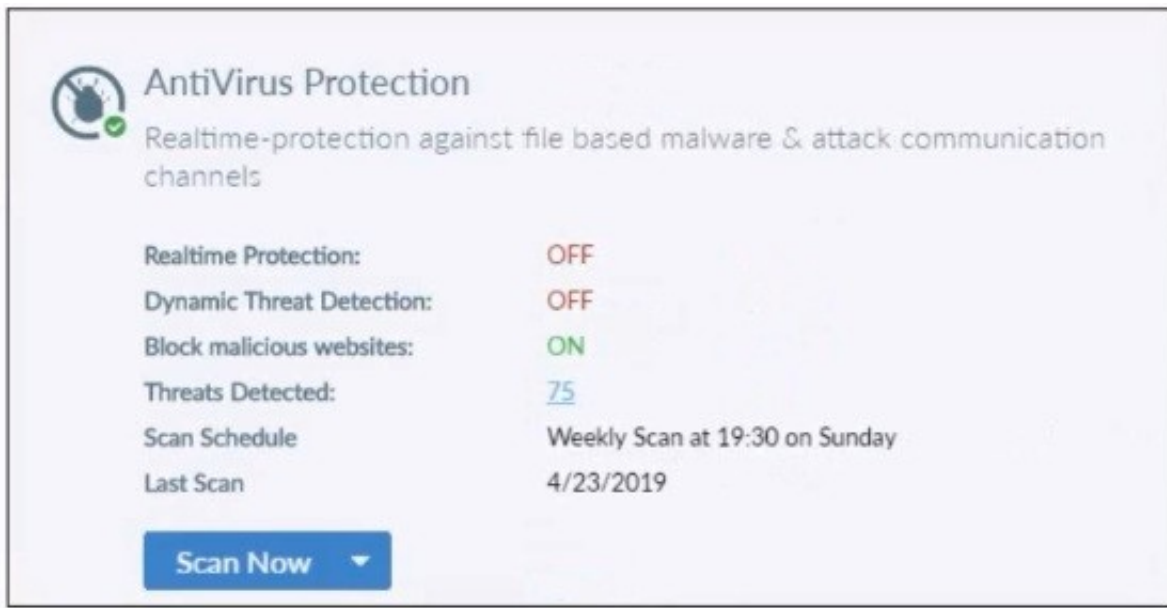
References

? FortiClient EMS 7.2 Study Guide, VPN Configuration Section

? Fortinet Documentation on Command Line Options for FortiClient VPN

NEW QUESTION 45

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 49

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 53

Refer to the exhibit.

```
config user fsso
  edit "Server"
    set type fortiems
    set server "10.0.1.200"
    set password ENC ebT9fHIMXIBykhWCSnG;P+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:

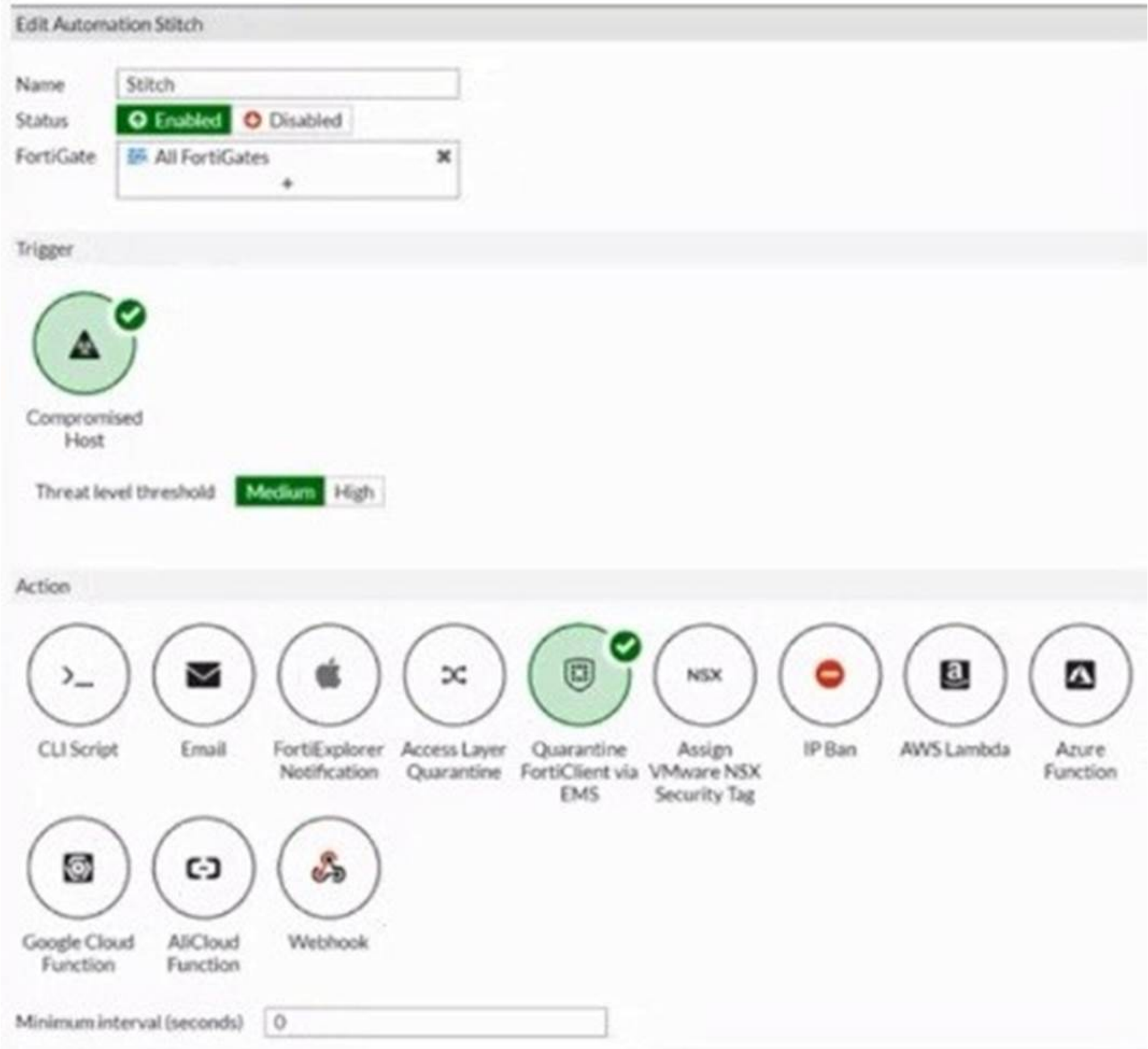
- ? The configuration shows the use of "type fortiems," indicating that FortiGate is set up to interact with FortiClient EMS.
 - ? The "server" field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.
 - ? The configuration includes an SSL-enabled connection, 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 55

Refer to the exhibit.



The screenshot shows the 'Edit Automation Stitch' configuration page. The 'Name' field is 'Stitch'. The 'Status' is 'Enabled'. The 'FortiGate' dropdown is set to 'All FortiGates'. The 'Trigger' section shows 'Compromised Host' with a 'Threat level threshold' set to 'Medium'. The 'Action' section shows a list of actions: CLI Script, Email, FortiExplorer Notification, Access Layer Quarantine, Quarantine FortiClient via EMS (selected), Assign VMware NSX Security Tag, IP Ban, AWS Lambda, and Azure Function. Below the actions, there are icons for Google Cloud Function, AllCloud Function, and Webhook. At the bottom, the 'Minimum interval (seconds)' is set to 0.

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.

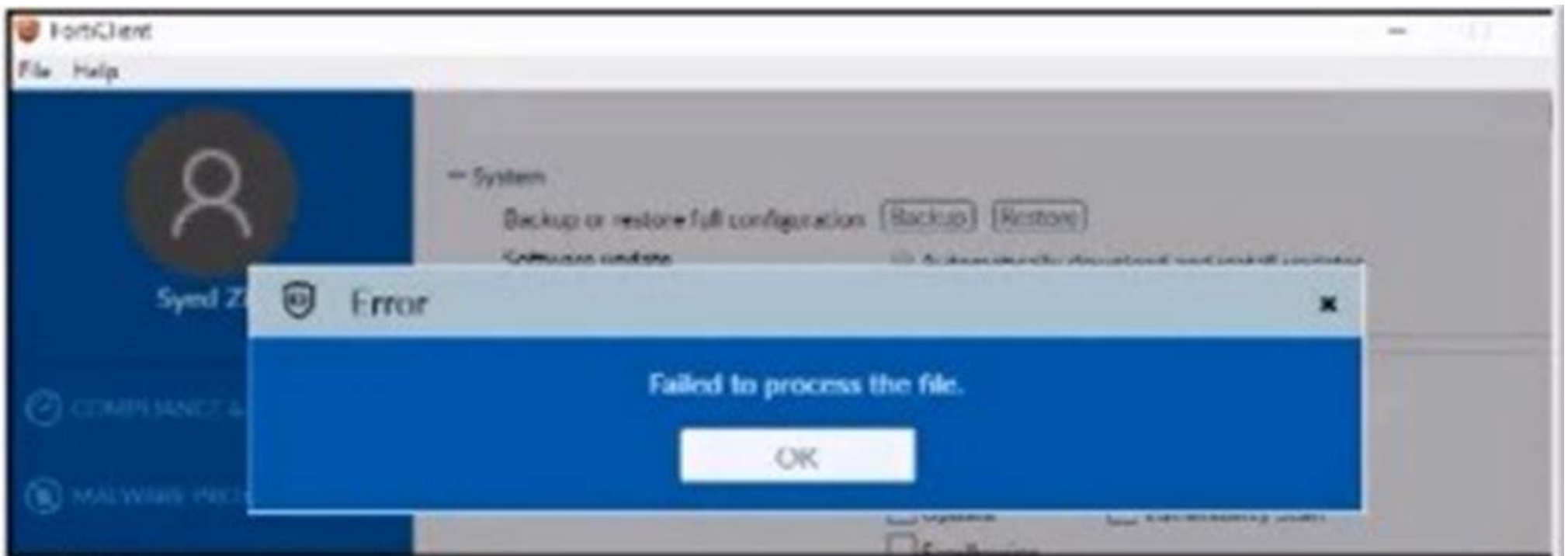
References

- ? FortiGate Security 7.2 Study Guide, Automation Stitches and Actions Section

? Fortinet Documentation on Configuring Automation Stitches and Quarantine Actions

NEW QUESTION 59

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_certificate>
  </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>
        </script>
      </on_disconnect>
    </connection>
  </connections>
</sslvpn>
```

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 61

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

Explanation:

? Simplifying Remote Access:

? Evaluating Access Control Methods:

? Conclusion:

References:

? ZTNA section in the FortiGate Infrastructure 7.2 Study Guide.

NEW QUESTION 65

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in 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 69

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FCT_AD-7.2 Practice Exam Features:

- * FCP_FCT_AD-7.2 Questions and Answers Updated Frequently
- * FCP_FCT_AD-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FCT_AD-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FCT_AD-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FCT_AD-7.2 Practice Test Here](#)