

# Fortinet

## Exam Questions FCP\_FCT\_AD-7.2

FCP-FortiClient EMS 7.2 Administrator



### NEW QUESTION 1

Which two are benefits of using multi-tenancy mode on FortiClient EMS? (Choose two.)

- A. Separate host servers manage each site.
- B. Licenses are shared among sites
- C. The fabric connector must use an IP address to connect to FortiClient EMS.
- D. It provides granular access and segmentation.

**Answer:** CD

#### Explanation:

? Understanding Multi-Tenancy Mode:

? Evaluating Benefits:

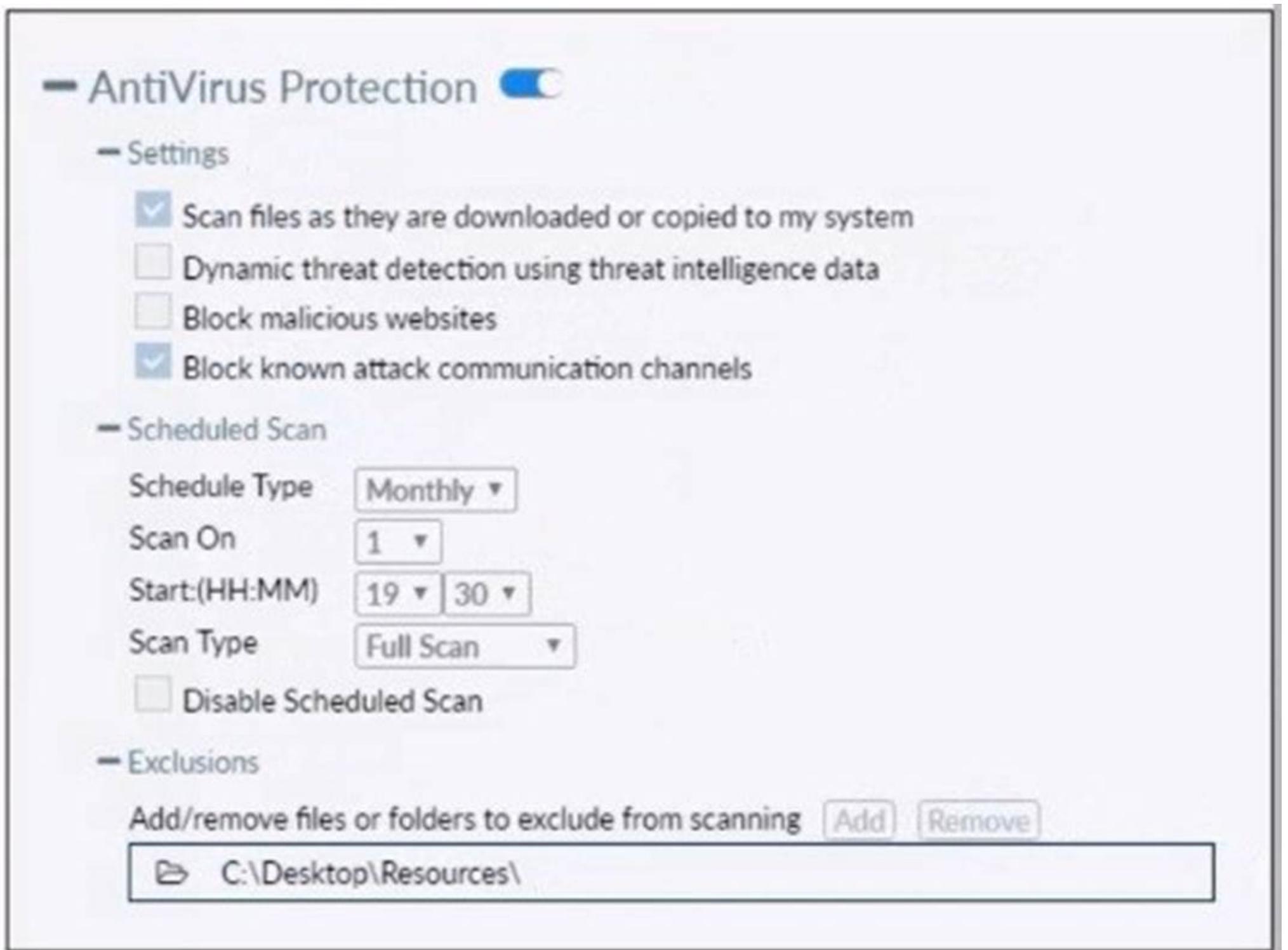
? Eliminating Incorrect Options:

References:

? FortiClient EMS multi-tenancy configuration and benefits documentation from the study guides.

### NEW QUESTION 2

Refer to the exhibit.



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 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**

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 5**

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 6**

An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?

- A. It redirects the client request to the access proxy.
- B. It uses the access proxy.
- C. It defines ZTNA server.
- D. It only uses ZTNA tags to control access for endpoints.

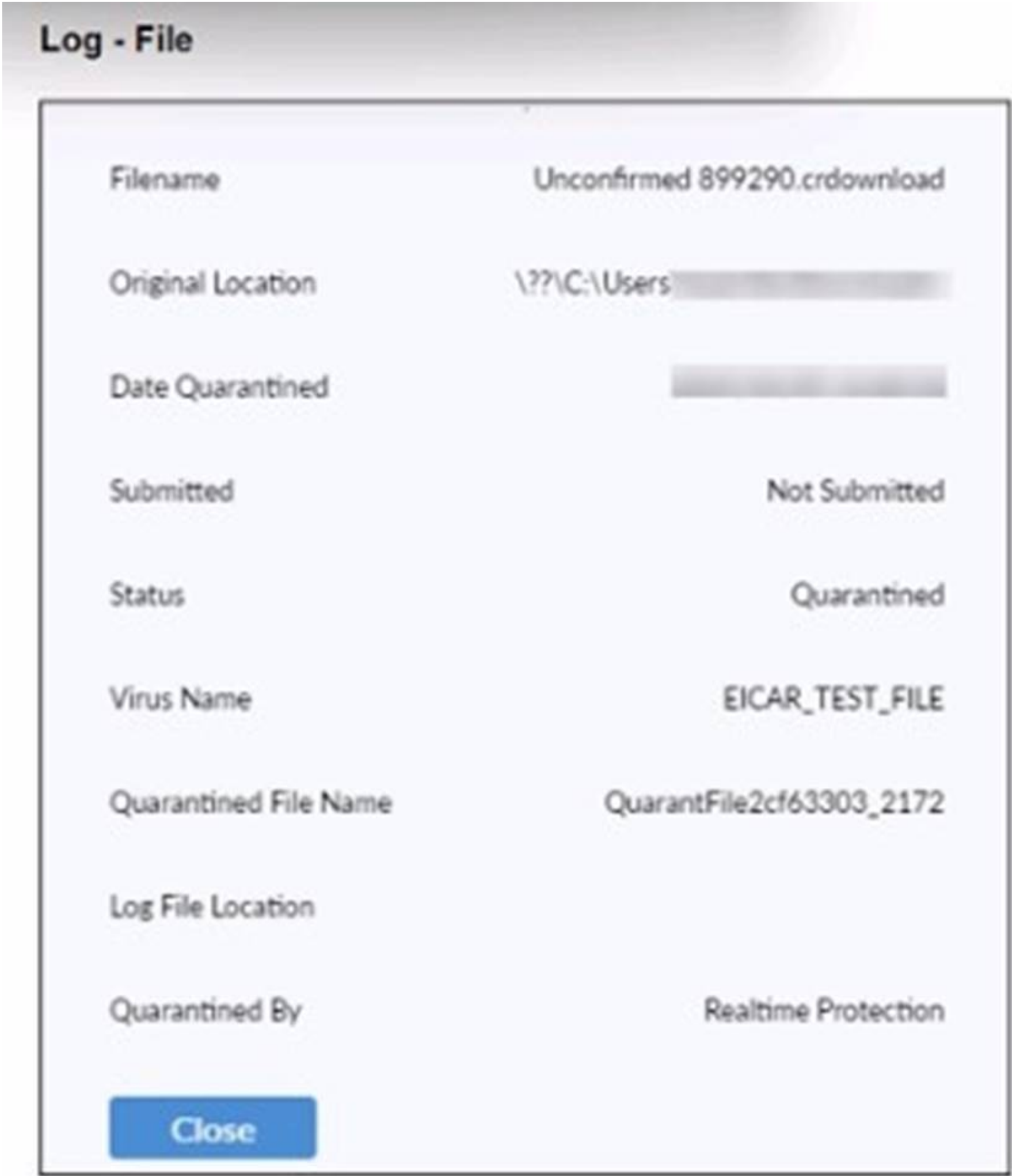
**Answer:** A

**Explanation:**

- "The firewall policy matches and redirects client requests to the access proxy VIP"<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration>

**NEW QUESTION 7**

Refer to the exhibit.



Based on the FortiClient tog details shown in the exhibit, which two statements ace true? (Choose two.)

- A. The filename Is Unconfirmed 899290.crdownload.
- B. The file status is Quarantined
- C. The filename is sent to FortiSandbox for further inspection.
- D. The file location is \\??\D:\Users\.

Answer: AB

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 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:**

**Explanation:**

Zero Trust Network Access (ZTNA) is a security architecture 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 10

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 11

FortiClient EMS endpoint policies

Endpoint Policies									
+ Add Change Priority Refresh Clear Filters Edit									
Name	Assigned Groups	Profile Components				Policy Components		Endpoint Count	Priority
Sales	All Groups trainingAD.training.lab	VPN Training	WEB Training	MW Training	FW Training	ZTNA Training	VULN Training	SB Training	SYS Training
Training	trainingAD.training.lab	VPN Training	WEB Training	MW Training	FW Training	ZTNA Training	VULN Training	SB Training	SYS Training
Default		VPN Default	WEB Default	MW Default	FW Default	ZTNA Default	VULN Default	SB Default	SYS Default

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 13


Refer to the exhibits.

## Security Fabric Settings

### ☒ FortiGate Telemetry


Security Fabric role Serve as Fabric Root Join Existing Fabric


Fabric name

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


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  ×

IP/Domain Name

Serial Number

Admin User

Password •••••••• Change

+



The screenshot shows the FortiGate Security Fabric settings for EMS integration. The fields are as follows:

- Hostname:** EMSServer
- Listen on IP:** 10.0.1.100
- Use FQDN:** ☒ (checked)
- FQDN:** myemsserver
- Remote HTTPS access:** ☐ (unchecked)
- SSL certificate:** No certificate imported

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

**Explanation:**

Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:

? Enable Remote HTTPS Access to EMS: This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate. Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

References

? FortiGate Infrastructure 7.2 Study Guide, Security Fabric and Integration with EMS Sections

? Fortinet Documentation on Enabling Remote HTTPS Access to FortiClient EMS

**NEW QUESTION 14**

Which two VPN types can a FortiClient endpoint user initiate 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 16**

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 21**  
Refer to the exhibit.

Edit Automation Stitch

Name

Stitch

Status

Enabled

Disabled

FortiGate

All FortiGates

Trigger

Compromised Host

Threat level threshold 

Medium

High

Action

CLI Script

Email

FortiExplorer Notification

Access Layer Quarantine

Quarantine FortiClient via EMS

NSX

Assign VMware NSX Security Tag

IP Ban

AWS Lambda

Azure Function

Google Cloud Function

AllCloud Function

Webhook

Minimum interval (seconds)

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 25**

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 29**

.....

## 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](#)**