

NSE5_FCT-7.0^{Q&As}

Fortinet NSE 5 - FortiClient EMS 7.0

Pass Fortinet NSE5_FCT-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse5_fct-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

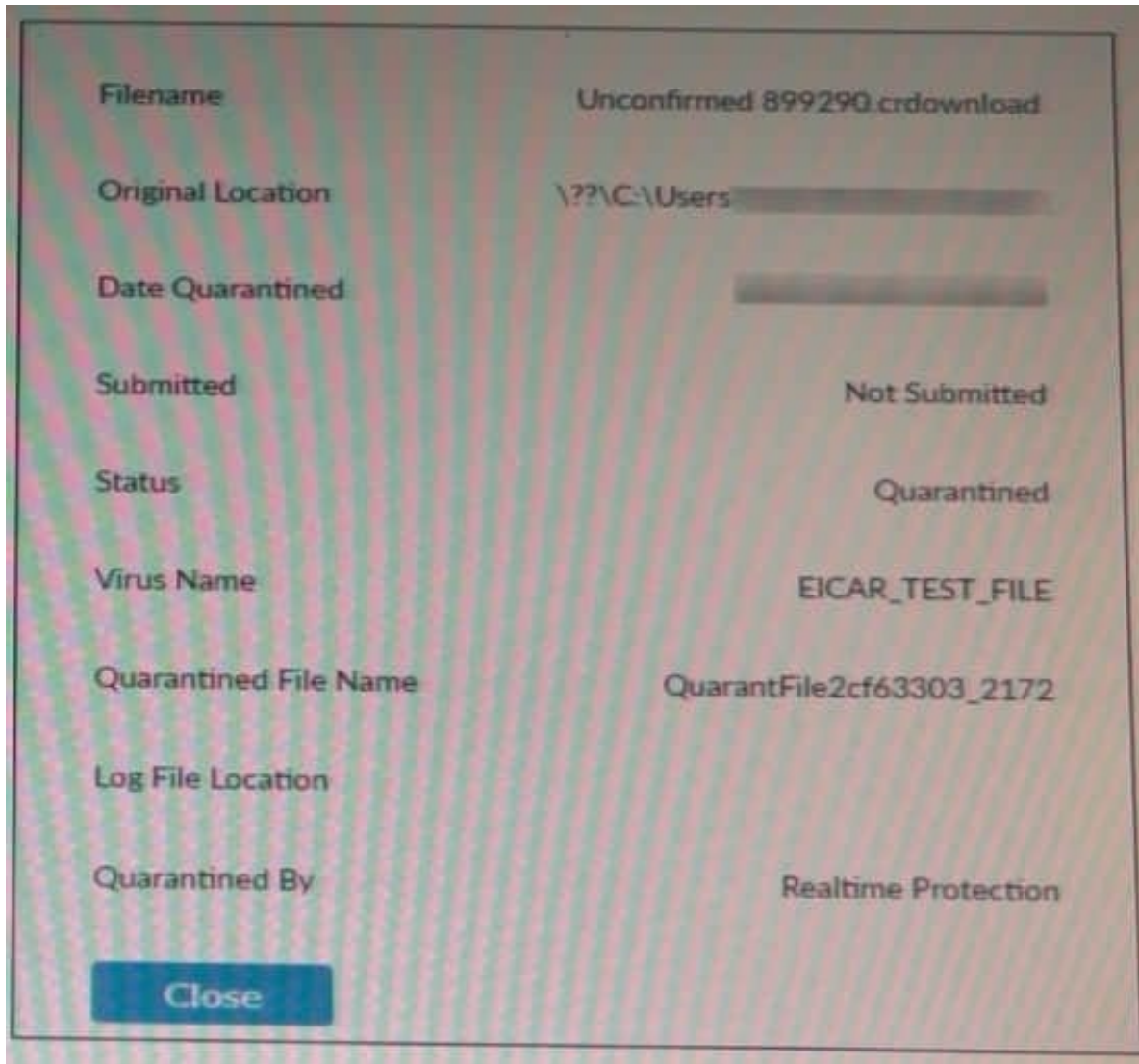
An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient dashboard. What must the administrator do to achieve this requirement?

- A. Disable select the vulnerability scan feature in the deployment package
- B. Use the default endpoint profile
- C. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
- D. Click the hide icon on the vulnerability scan tab

Correct Answer: D

QUESTION 2

Refer to the exhibit.



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

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

Correct Answer: AD

QUESTION 3

In a FortiSandbox integration, what does the remediation option do?

- A. Wait for FortiSandbox results before allowing files

- B. Exclude specified files
- C. Alert and notify only
- D. Deny access to a file when it sees no results

Correct Answer: C

QUESTION 4


Refer to the exhibit.

Log Details

General

Absolute Date/Time 2021/11/25 08:59:18
Time 08:59:18
Duration 0s
Session ID 6308
Virtual Domain root

Source

IP 100.64.2.253
Source Port 49964
Country/Region Reserved
Source Interface  port1
User

Destination

IP 100.64.1.10
Port 9443
Country/Region Reserved
Destination Interface root


Application Control

Application Name
Category unscanned
Risk undefined
Protocol 6
Service tcp/9443

Data

Received Bytes 0 B
Received Packets 0
Sent Bytes 0 B
Sent Packets 0
Message Denied: failed to match an API-gateway

Action

Action Deny: policy violation
Security Action  Blocked
Policy ID ZTNA-WAN (4)
Policy UUID 23f88b34-4e0b-51ec-0e83-dab1019c2d5c
Policy Type Firewall

Which shows the output of the ZTNA traffic log on FortiGate. What can you conclude from the log message?

- A. The remote user connection does not match the explicit proxy policy.
- B. The remote user connection does not match the ZTNA server configuration.
- C. The remote user connection does not match the ZTNA rule configuration.
- D. The remote user connection does not match the ZTNA firewall policy

Correct Answer: B

API gateway cannot be matched or real servers cannot be reached

QUESTION 5

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

- A. It enforces access control
- B. It redirects the client request to the access proxy
- C. It defines the access proxy
- D. It applies security profiles to protect traffic

Correct Answer: AD

"A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic."

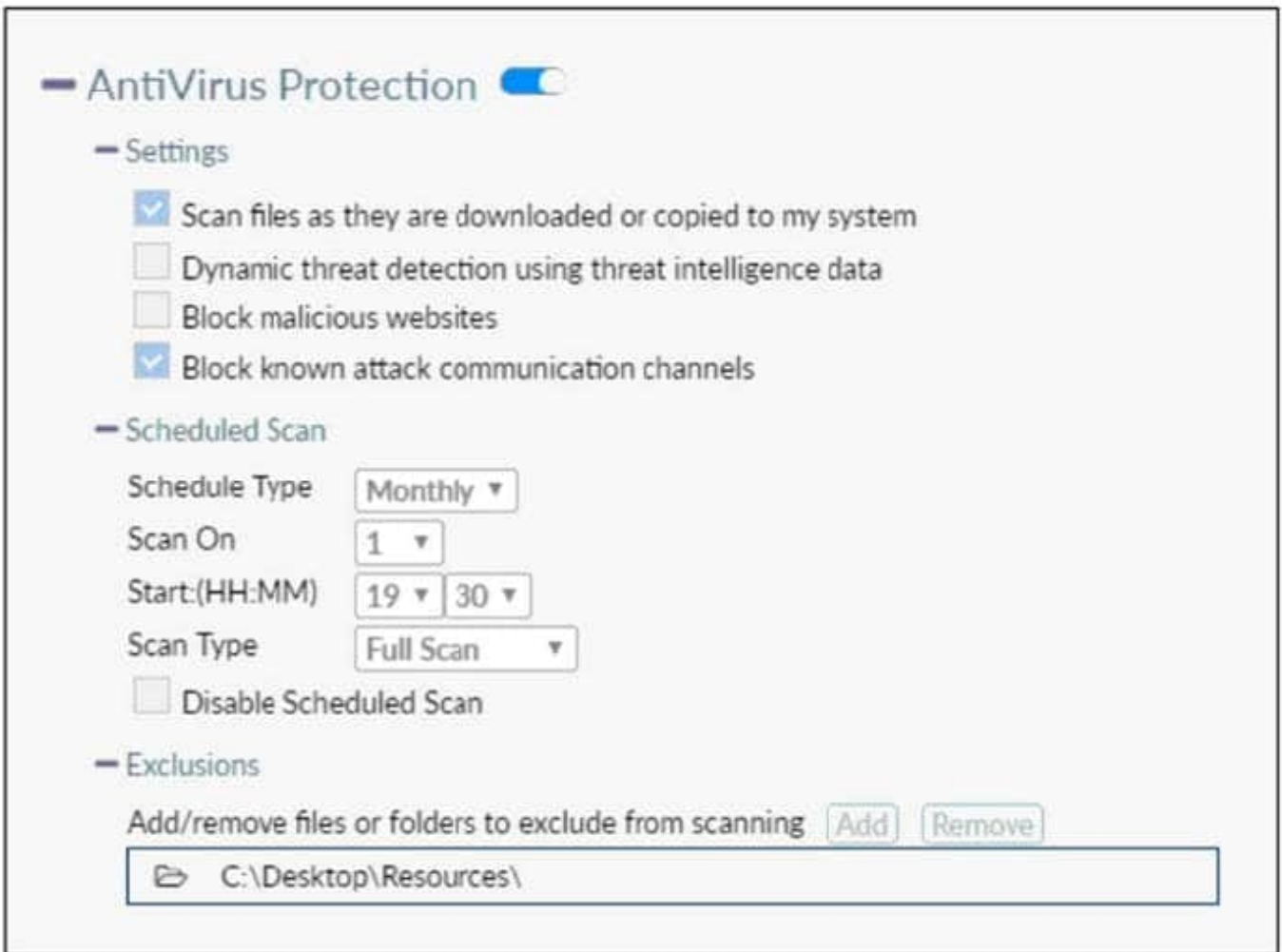
"ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security

profiles to scan the traffic."

<https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access>

QUESTION 6

Refer to the exhibit.



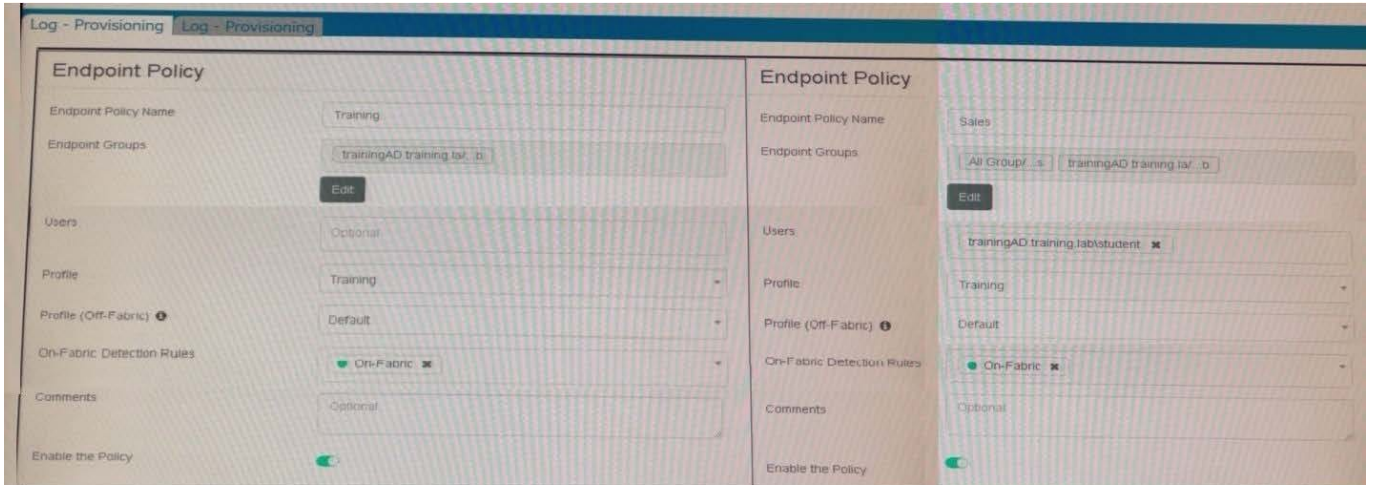
Based on the settings shown in the exhibit which statement about FortiClient behavior is true?

- 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.

Correct Answer: A

QUESTION 7

Refer to the exhibits.



Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Priority	Enabled
Training	trainingAD.training.lab	PROFILE: Training OFF-FABRIC: Default	ON-FABRIC: On-Fabric	1	1	Yes
Sales	All Groups trainingAD.training.lab	PROFILE: Training OFF-FABRIC: Default	ON-FABRIC: On-Fabric	1	2	Yes
Default		PROFILE: Training OFF-FABRIC: Default	ON-FABRIC: On-Fabric	0	0	No

Which shows the configuration of endpoint policies.

Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

- A. FortiClient EMS will assign the Sales policy
- B. FortiClient EMS will assign the Training policy
- C. FortiClient EMS will assign the Default policy
- D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Correct Answer: B

QUESTION 8

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

- A. L2TP
- B. IPsec
- C. DLP
- D. Vulnerability management

E. Real-time protection

Correct Answer: BDE

QUESTION 9

An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate. What is the prerequisite to get FortiClient EMS to connect to FortiGate successfully?

- A. Revoke and update the FortiClient EMS root CA.
- B. Revoke and update the FortiClient client certificate on EMS.
- C. Import and verify the FortiClient client certificate on FortiGate.
- D. Import and verify the FortiClient EMS root CA certificate on FortiGate

Correct Answer: D

QUESTION 10

What action does FortiClient anti-exploit detection take when it detects exploits?

- A. Blocks memory allocation to the compromised application process
- B. Patches the compromised application process
- C. Deletes the compromised application process
- D. Terminates the compromised application process

Correct Answer: D

The anti-exploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.

[Latest NSE5_FCT-7.0 Dumps](#)

[NSE5_FCT-7.0 PDF Dumps](#) [NSE5_FCT-7.0 VCE Dumps](#)