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.certbus.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

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.

QUESTION 2

Refer to the exhibit.

Log - Policy

```
1:40:39 PM    Information    Vulnerability   id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM    Information    Vulnerability   id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM    Information    ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:12:22 PM    Information    Config  id=96882 msg="Policy 'Default' was received and applied"
2:13:27 PM    Information    ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:14:32 PM    Information    ESNAC   id=96959 emshostname=WIN-EHVKBEA3S71 msg="Endpoint has AV whitelist engine version 6.00134 and si
2:14:54 PM    Information    Config  id=96882 msg="Policy 'Default' was received and applied"
2:16:01 PM    Information    ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:20:19 PM    Information    Config  id=96883 msg="Compliance rules 'default' were received and applied"
2:20:23 PM    Debug   ESNAC   PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
2:20:23 PM    Debug   ESNAC   cb828898d1ae56916f84cc7909a1eb1a
2:20:23 PM    Debug   ESNAC   Before Reload Config
2:20:23 PM    Debug   ESNAC   ReloadConfig
2:20:23 PM    Debug   Scheduler       stop_task() called
2:20:23 PM    Debug   Scheduler       GUI change event
2:20:23 PM    Debug   Scheduler       stop_task() called
2:20:23 PM    Information    Config  id=96882 msg="Policy 'Fortinet-Training' was received and applied"
2:20:23 PM    Debug   Config  'scan on registration' is disabled - delete 'on registration' vulnerability scan.
2:20:23 PM    Debug   Config  ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.
```

Based on the FortiClient logs shown in the exhibit which endpoint profile policy is currently applied to the FortiClient endpoint from the EMS server?

A. Default

B. Compliance rules default

C. Fortinet- Training

D. Default configuration policy

Correct Answer: C

QUESTION 3

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

A. FortiGate

B. FortiGate Access Proxy

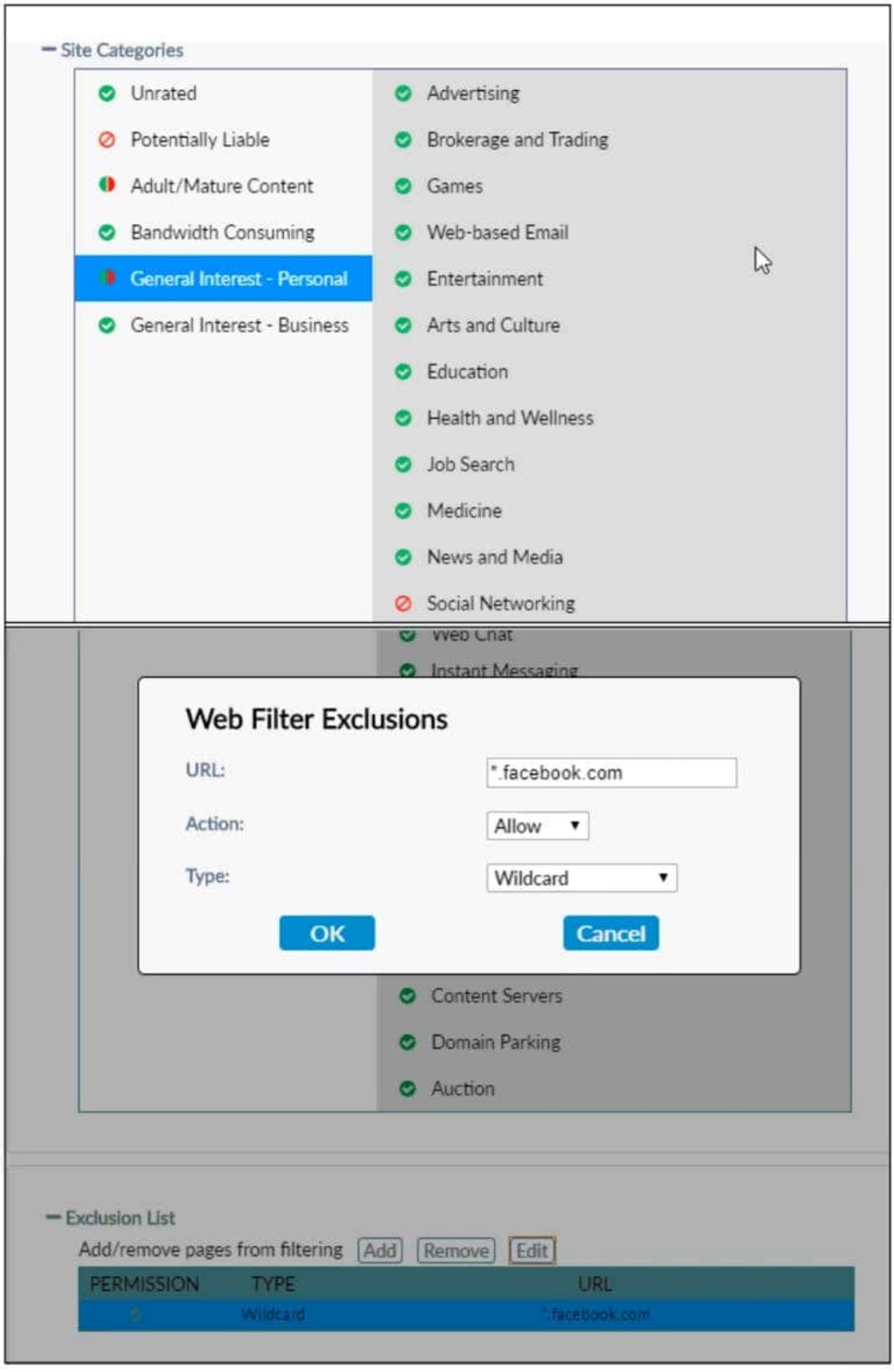
C. FortiClient

D. FortiClient EMS

Correct Answer: D

QUESTION 4

Refer to the exhibit.


Site Categories
Unrated
Potentially Liable
Adult/Mature Content
Bandwidth Consuming
General Interest - Personal
General Interest - Business
Advertising
Brokerage and Trading
Games
Web-based Email
Entertainment
Arts and Culture
Education
Health and Wellness
Job Search
Medicine
News and Media
Social Networking
Web Filter Exclusions
URL:
*.facebook.com
Action:
Allow
Type:
Wildcard
OK
Cancel
Content Servers
Domain Parking
Auction
Exclusion List
Add/remove pages from filtering
Add
Remove
Edit
PERMISSION
TYPE
URL
Wildcard
*.facebook.com

Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www.facebook.com?

A. FortiClient will monitor only the user\\'s web access to the Facebook website

B. FortiClient will block access to Facebook and its subdomains.

C. FortiClient will prompt a warning message to warn the user before they can access the Facebook website

D. FortiClient will allow access to Facebook.

Correct Answer: D

QUESTION 5

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

Correct Answer: C

QUESTION 6

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 7

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

A. Wait for FortiSandbox results before allowing files

B. Exclude specified files

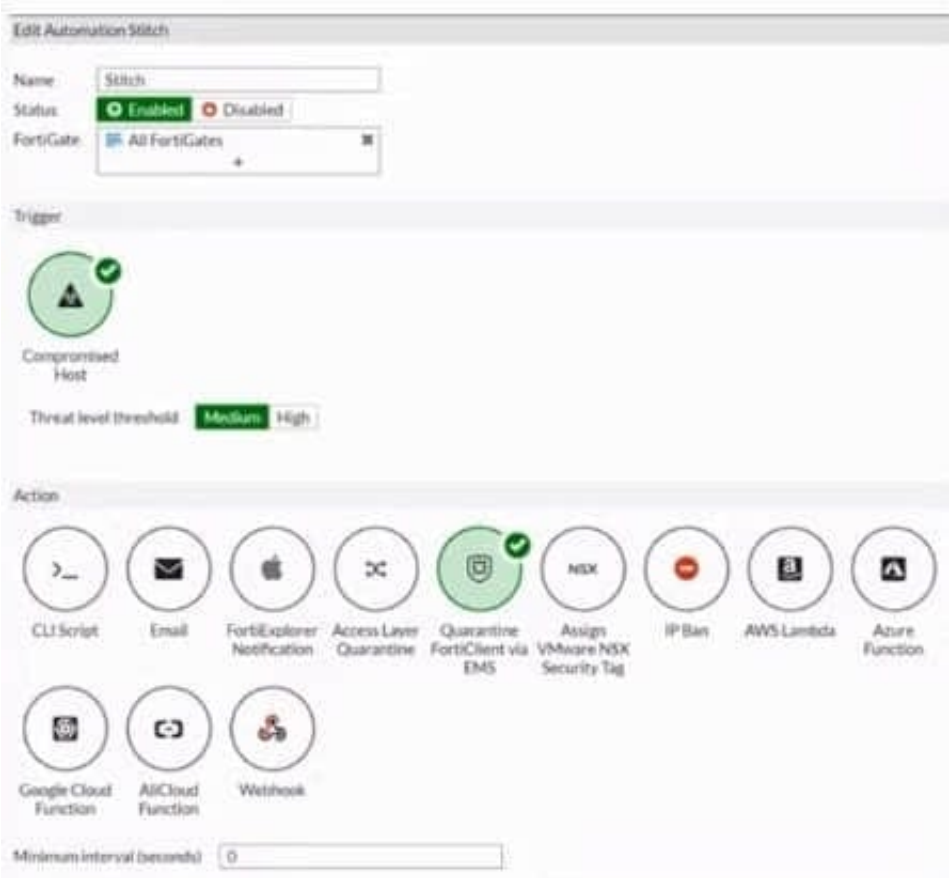
C. Alert and notify only

D. Deny access to a file when it sees no results

Correct Answer: C

QUESTION 8

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

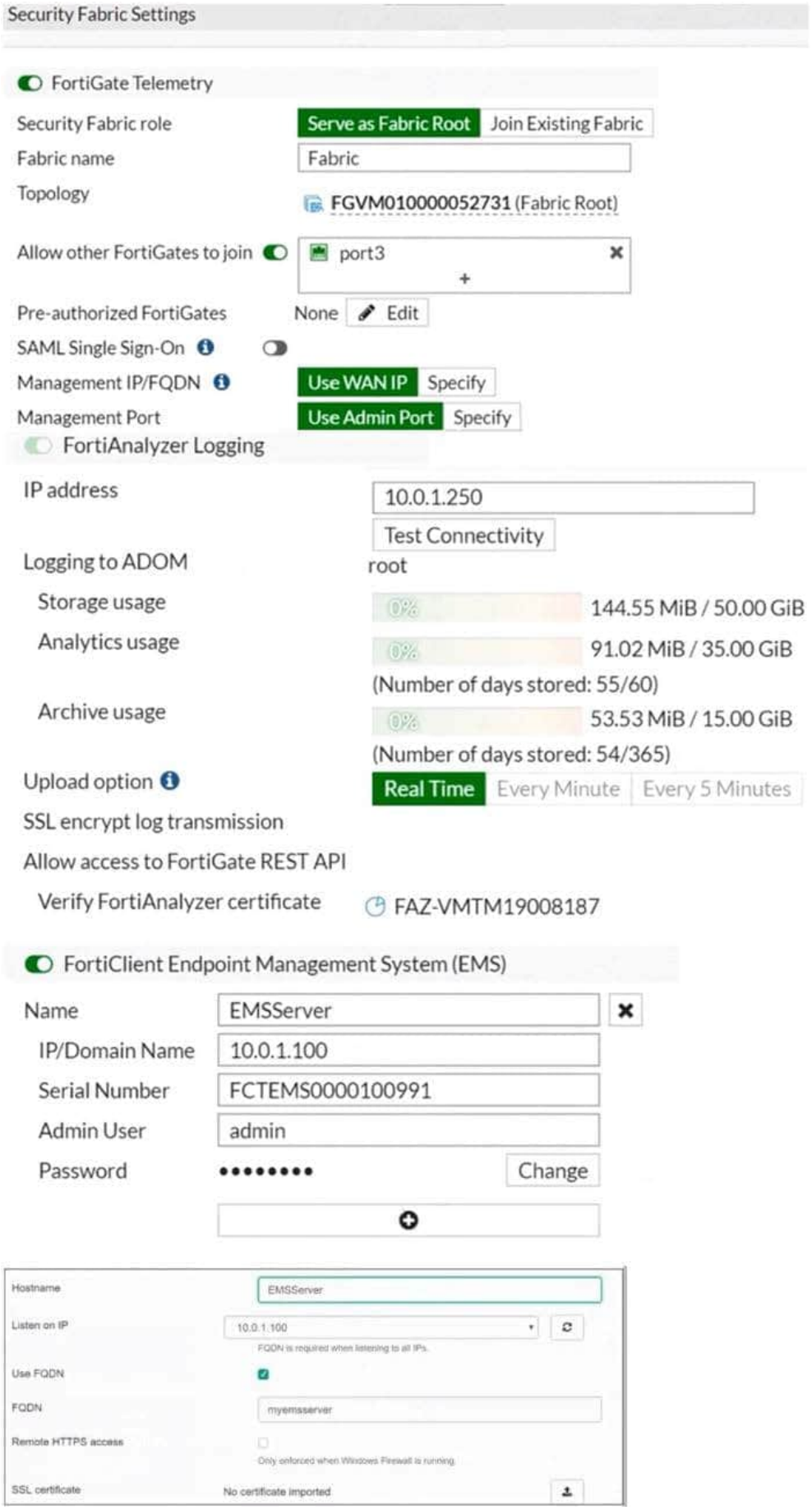
C. An email notification will be sent for compromised endpoints

D. Endpoints will be quarantined through FortiSwitch

Correct Answer: A

QUESTION 9

Refer to the exhibits.


Security Fabric Settings
FortiGate Telemetry
Security Fabric role
Serve as Fabric Root
Join Existing Fabric
Fabric name
Fabric
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
10.0.1.250
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
EMSServer
IP/Domain Name
10.0.1.100
Serial Number
FCTEMS0000100991
Admin User
admin
Password
Change
Hostname
EMSServer
Listen on IP
10.0.1.100
FQDN is required when listening to all IPs.
Use FQDN
FQDN
myemsserver
Remote HTTPS access
Only enforced when Windows Firewall is running.
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.

Correct Answer: A

QUESTION 10

When site categories are disabled in FortiClient webfilter and antivirus (malicious websites), which feature can be used to protect the endpoint from malicious web access?

A. Real-time protection list

B. Block malicious websites on antivirus

C. FortiSandbox URL list

D. Web exclusion list

Correct Answer: D