



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.passapply.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 inventory on the endpoints. without showing the feature on the FortiClient dashboard What must the administrator do to achieve this requirement?

- A. The administrator must use default endpoint profile
- B. The administrator must not select the vulnerability scan feature in the deployment package.
- C. The administrator must select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
- D. The administrator must click the hide icon on the vulnerability scan tab

Correct Answer: D

QUESTION 2

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 software application is blocked by the application firewall?

- A. Twitter
- B. Facebook
- C. Internet Explorer
- D. Firefox

Correct Answer: D



QUESTION 3

Refer to the exhibit.

Edit Automation Switch

Name: Switch

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, Assign VMware NSX Security Tag, IP Ban, AWS Lambda, Azure Function, Google Cloud Function, AliCloud 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

Correct Answer: A

QUESTION 4

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 5

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

[Latest NSE5_FCT-7.0 Dumps](#)

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