NSE5_FCT-6.2^Q&As^

Fortinet NSE 5 - FortiClient EMS 6.2

Pass Fortinet NSE5_FCT-6.2 Exam with 100% Guarantee

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.

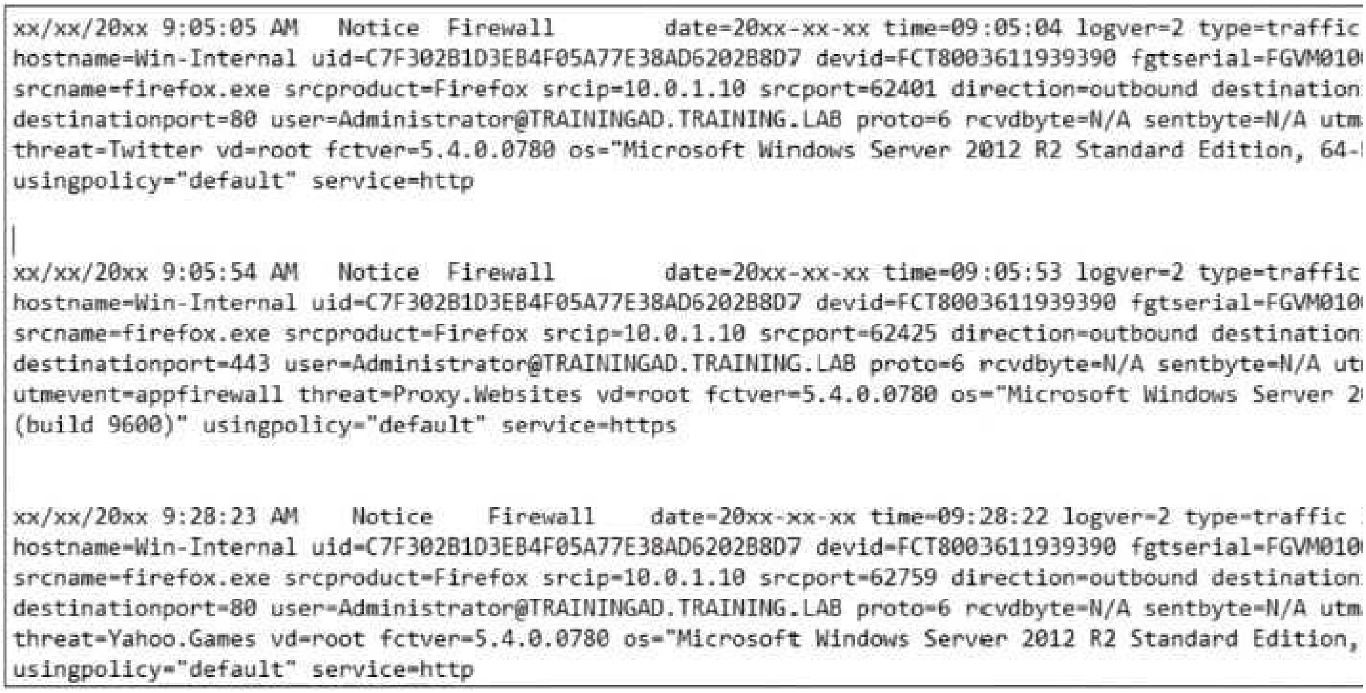
C. The administrator must select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile

D. The administrator must click the hide icon on the vulnerability scan tab

Correct Answer: C

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
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destination
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utm
threat=Twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-
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
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destination
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A ut
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2
(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
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destination
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utm
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition,
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

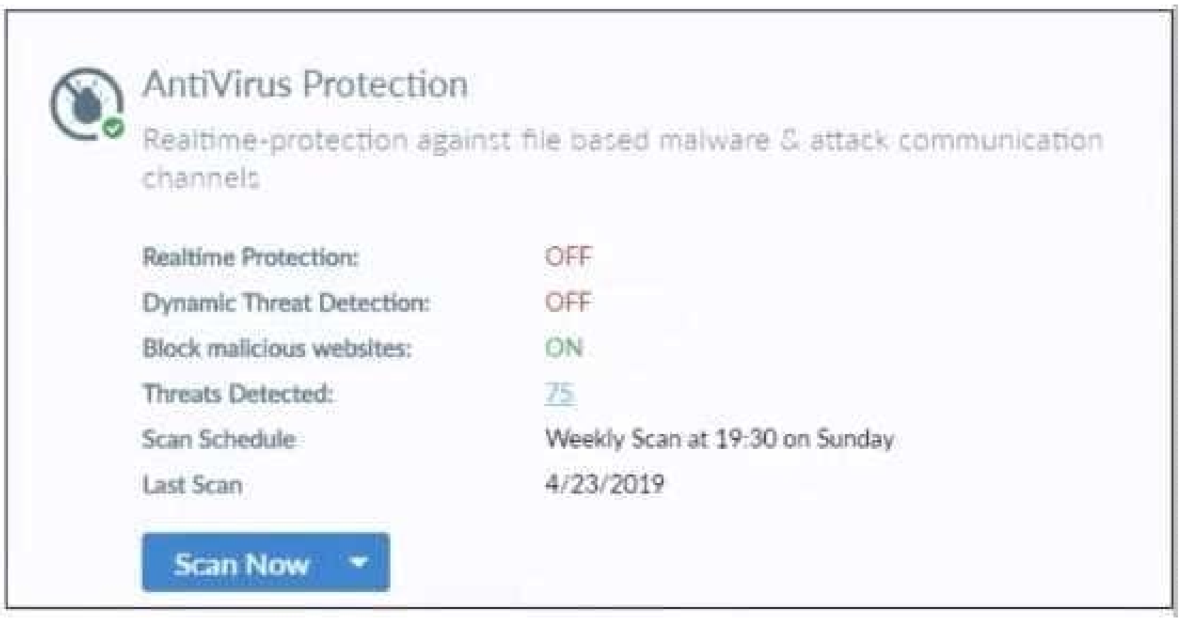
C. Internet Explorer

D. Firefox

Correct Answer: D

QUESTION 3

Refer to the exhibit.



AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Realtime Protection:	OFF
Dynamic Threat Detection:	OFF
Block malicious websites:	ON
Threats Detected:	75
Scan Schedule	Weekly Scan at 19:30 on Sunday
Last Scan	4/23/2019

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

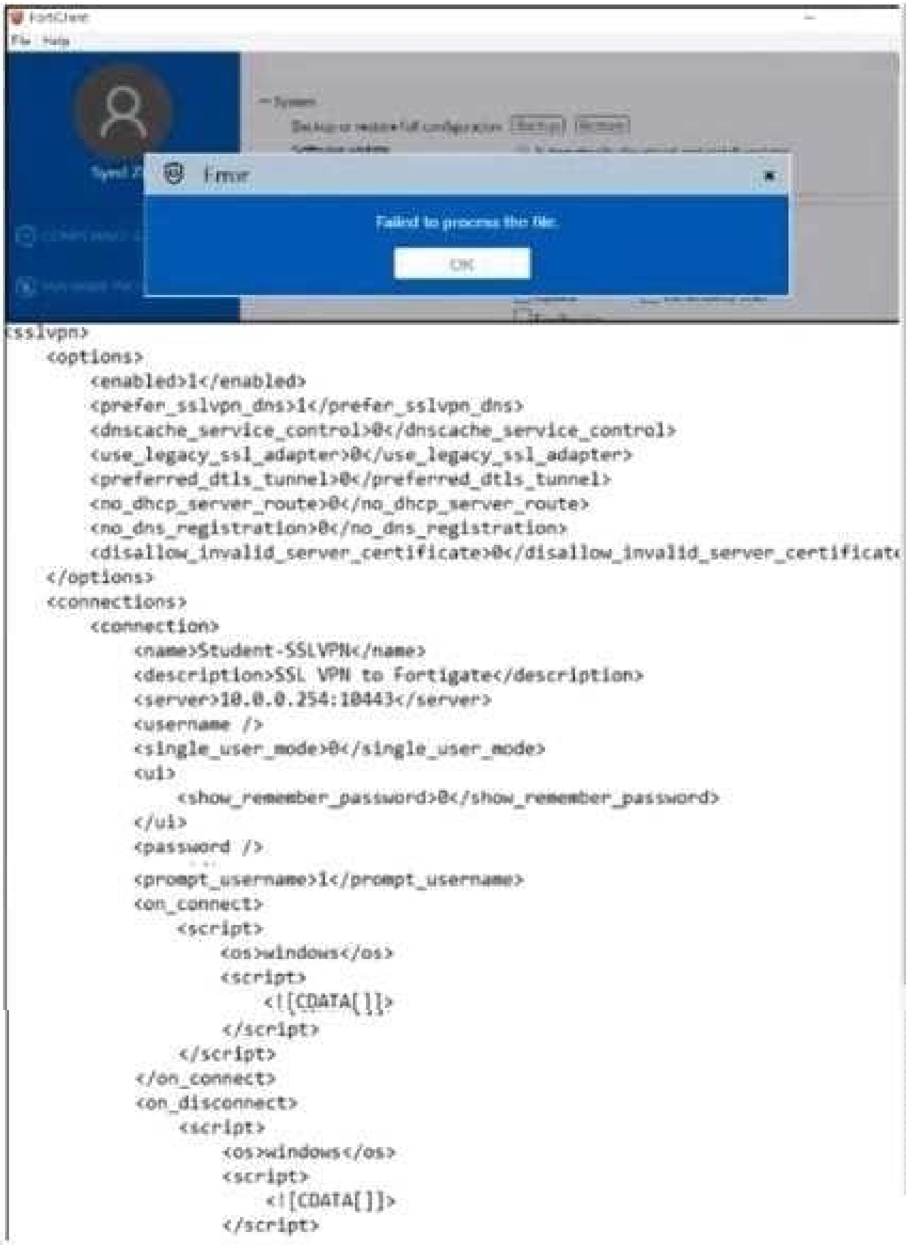
C. Sends the infected file to FortiGuard for analysis

D. Allows the infected file to download without scan

Correct Answer: D

QUESTION 4

Refer to the exhibit.



Error

Failed to process the file.

```
<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_certificat
    </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>
```

A. An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit

B. Based on the XML settings shown in the exhibit, what must the administrator do to resolve the issue with the XML configuration file?

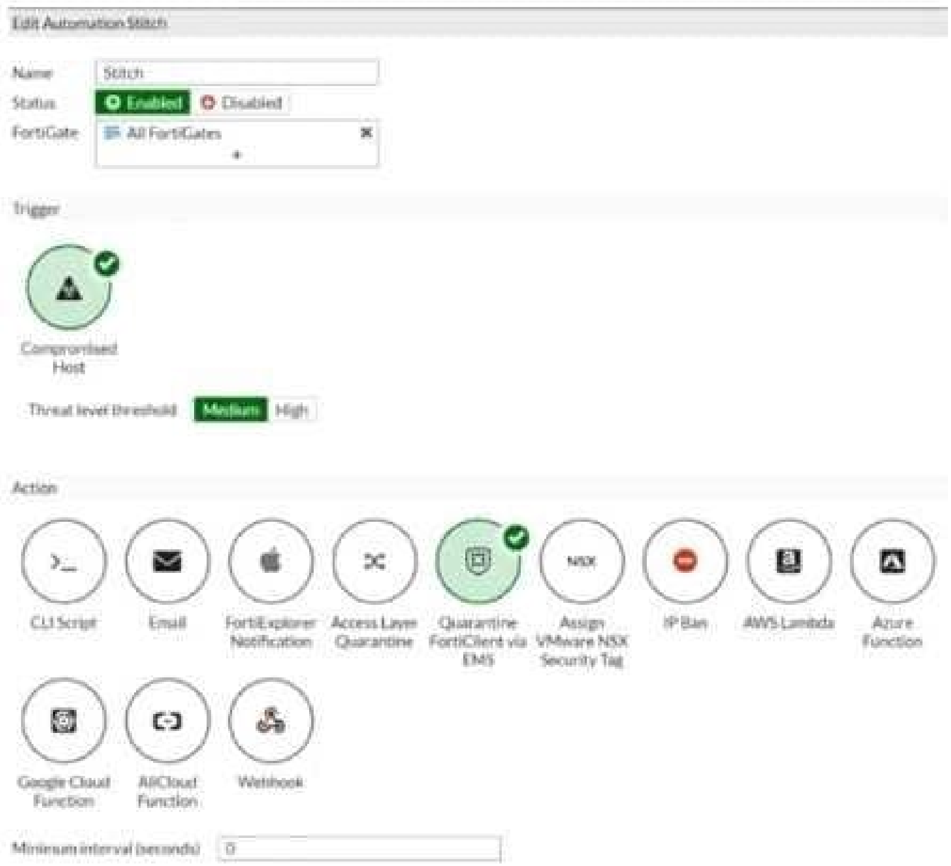
C. The administrator must resolve the XML syntax error. The administrator must use a password to decrypt the file The administrator must change the file size

D. The administrator must save the file as FortiClient-config conf.

Correct Answer: A

QUESTION 5

Refer to the exhibit.



Edit Automation Stitch

Name: Stitch

Status: ● Enabled ○ Disabled

FortiGate: All FortiGates

Trigger

Compromised Host

Threat level threshold: [✓ Medium] High

Action

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

Latest NSE5_FCT-6.2 Dumps NSE5_FCT-6.2 PDF Dumps NSE5_FCT-6.2 VCE Dumps