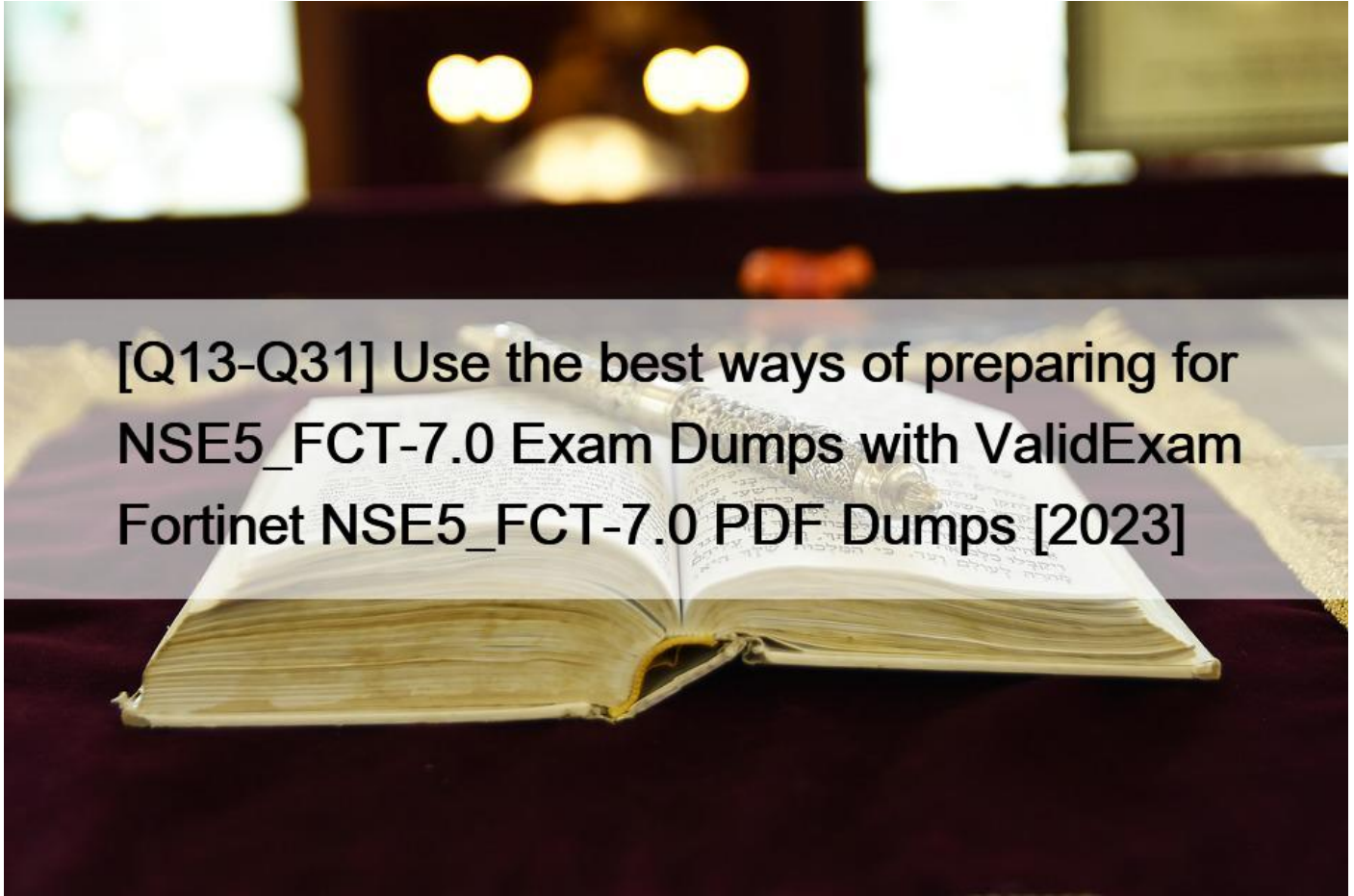


[Q13-Q31] Use the best ways of preparing for NSE5_FCT-7.0 Exam Dumps with ValidExam Fortinet NSE5_FCT-7.0 PDF Dumps [2023]



Use the best ways of preparing for NSE5_FCT-7.0 Exam Dumps with ValidExam Fortinet NSE5_FCT-7.0 dump PDF [2023 Fortinet NSE5_FCT-7.0 exam candidates will surely pass the Exam if they consider the NSE5_FCT-7.0 dumps learning material presented by ValidExam. Q13. An administrator installs FortiClient on Windows Server.

What is the default behavior of real-time protection control?

- * Real-time protection must update AV signature database
- * Real-time protection sends malicious files to FortiSandbox when the file is not detected locally
- * Real-time protection is disabled
- * Real-time protection must update the signature database from FortiSandbox

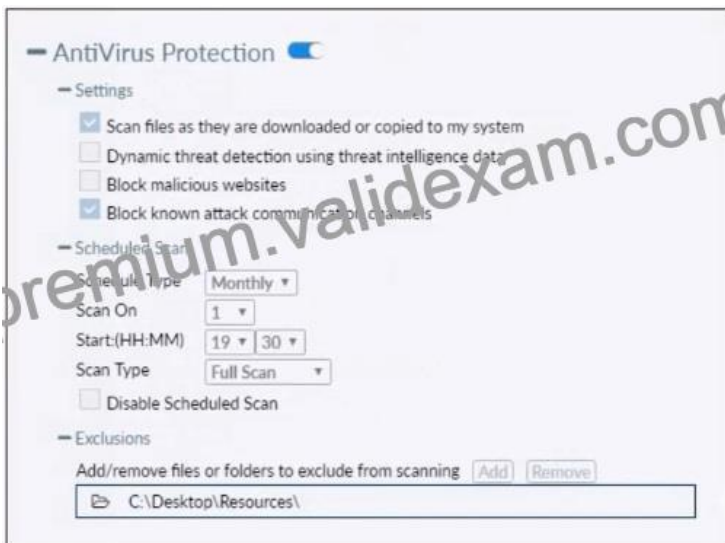
Q14. Refer to the exhibit.

```
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 cb82889811ae56916f84cc7909a1eb1a
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?

- * Default
- * Compliance rules default
- * Fortinet- Training
- * Default configuration policy

Q15. Refer to the exhibit.



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

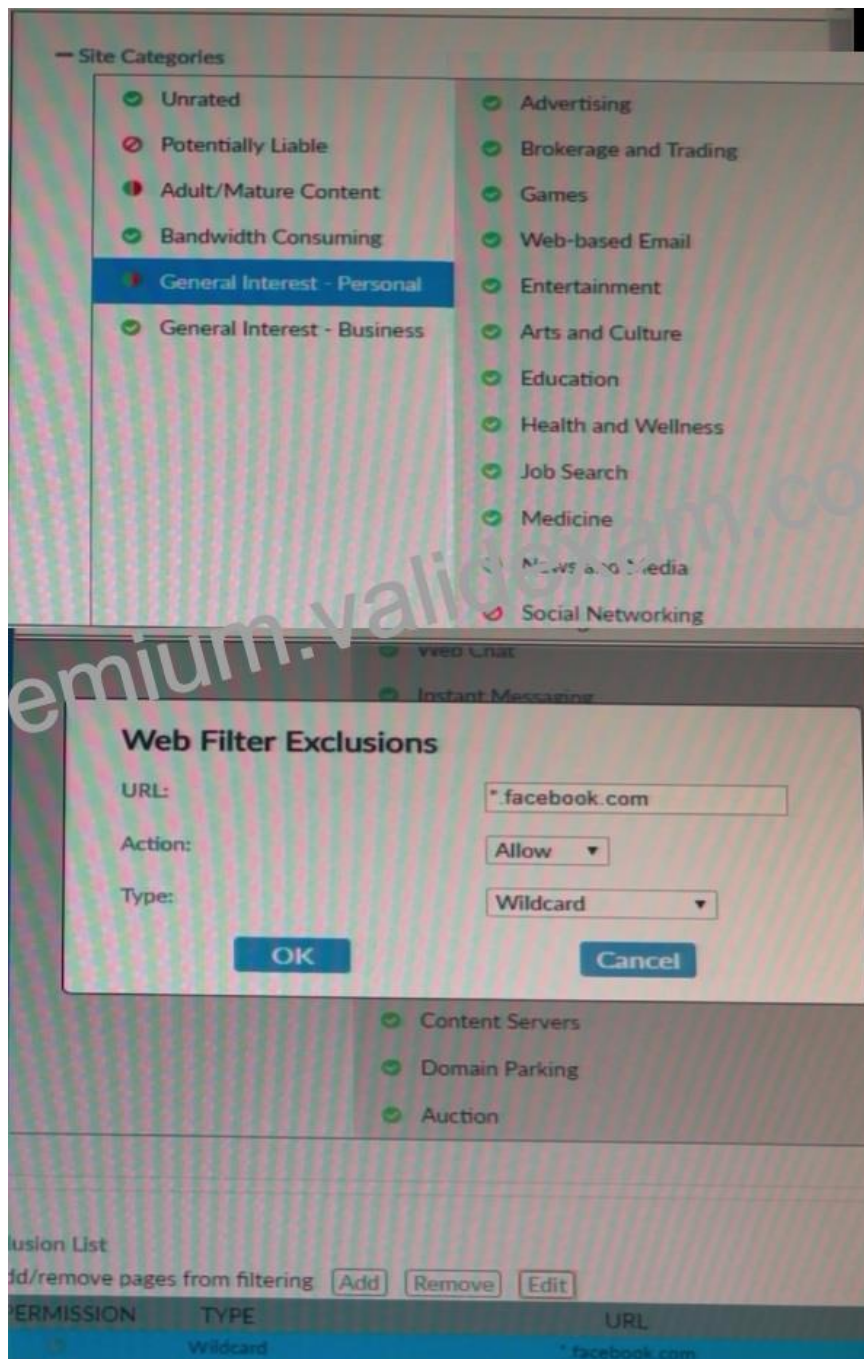
- * FortiClient quarantines infected files and reviews later, after scanning them.
- * FortiClient blocks and deletes infected files after scanning them.
- * FortiClient scans infected files when the user copies files to the Resources folder
- * FortiClient copies infected files to the Resources folder without scanning them.

Q16. What does FortiClient do as a fabric agent? (Choose two.)

- * Provides IOC verdicts

- * Automates Responses
- * Creates dynamic policies

Q17. Refer to the exhibit.



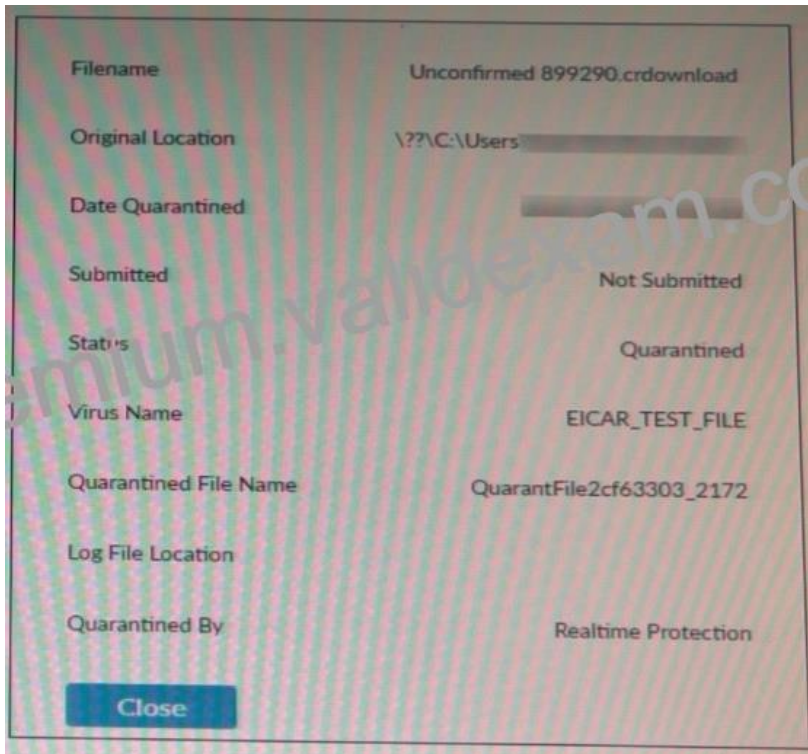
Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www.facebook.com?

- * FortiClient will allow access to Facebook
- * FortiClient will monitor only the user's web access to the Facebook website
- * FortiClient will block access to Facebook and its subdomains.
- * FortiClient will prompt a warning message to warn the user before they can access the Facebook website

Q18. 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?

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

Q19. Refer to the exhibit.



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

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

Q20. Which three types of antivirus scans are available on FortiClient? (Choose three)

- * Proxy scan
- * Full scan
- * Custom scan
- * Flow scan
- * Quick scan

Q21. 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_Sites 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?

- * Twitter
- * Facebook
- * Internet Explorer
- * Firefox

Q22. Refer to the exhibit.

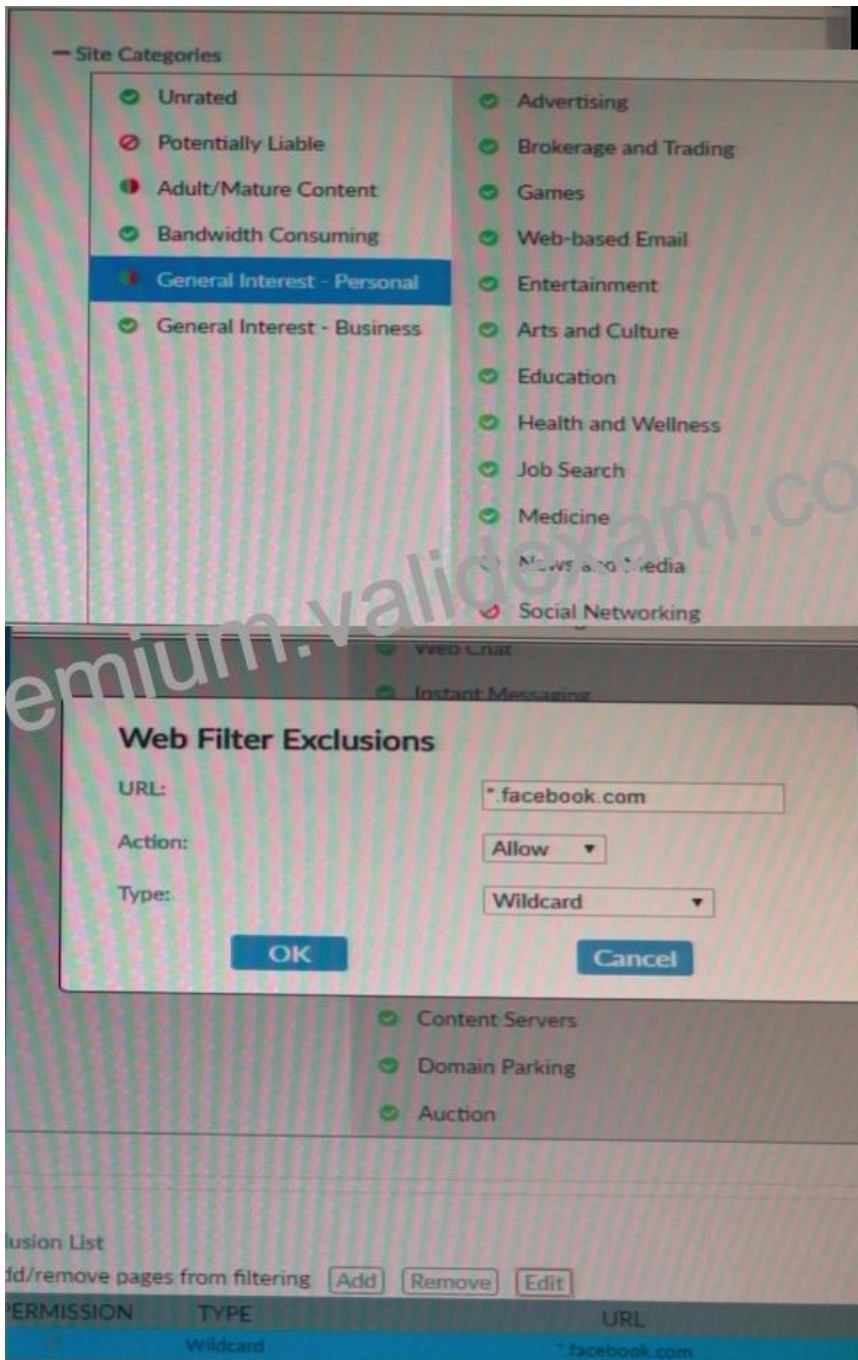
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time
Deployment-1	All Groups	First-Time Installation	
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade	

Which shows FortiClient EMS deployment profiles.

When an administrator creates a deployment profile on FortiClient EMS, which statement about the deployment profile is true?

- * Deployment-1 will install FortiClient on new AD group endpoints
- * Deployment-2 will install FortiClient on both the AD group and workgroup
- * Deployment-2 will upgrade FortiClient on both the AD group and workgroup
- * Deployment-1 will upgrade FortiClient only on the workgroup

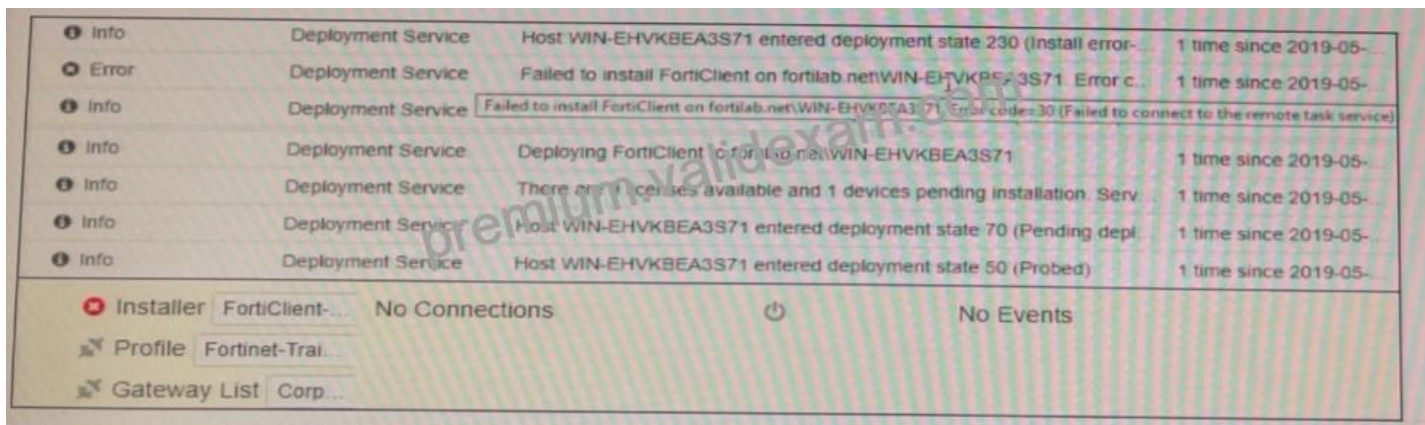
Q23. Refer to the exhibit.



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

- * FortiClient will allow access to Facebook
- * FortiClient will monitor only the user's web access to the Facebook website
- * FortiClient will block access to Facebook and its subdomains.
- * FortiClient will prompt a warning message to warn the user before they can access the Facebook website

Q24. Refer to the exhibit.



Based on the logs shown in the exhibit, why did FortiClient EMS fail to install FortiClient on the endpoint?

- * The remote registry service is not running
- * The Windows installer service is not running
- * The task scheduler service is not running.
- * The FortiClient antivirus service is not running

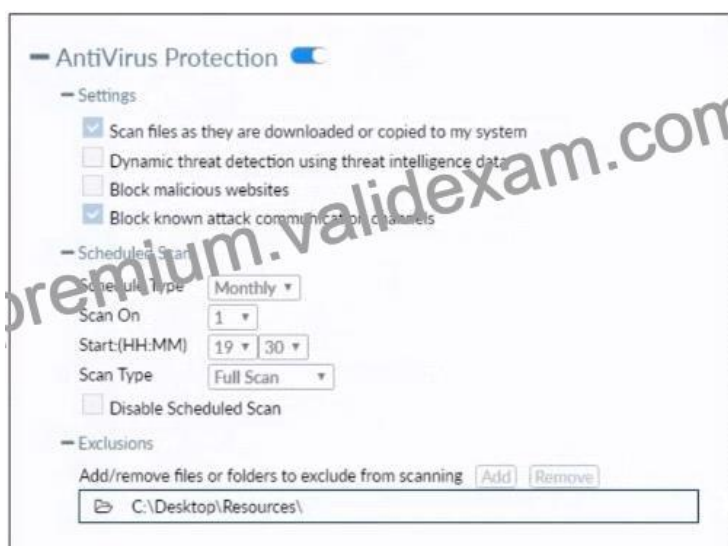
Q25. Which component or device shares ZTNA tag information through Security Fabric integration?

- * FortiGate
- * FortiGate Access Proxy
- * FortiClient

Q26. What is the function of the quick scan option on FortiClient?

- * It scans programs and drivers that are currently running, for threats.
- * It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
- * It performs a full system scan including all files, executable files, DLLs, and drivers for threats.

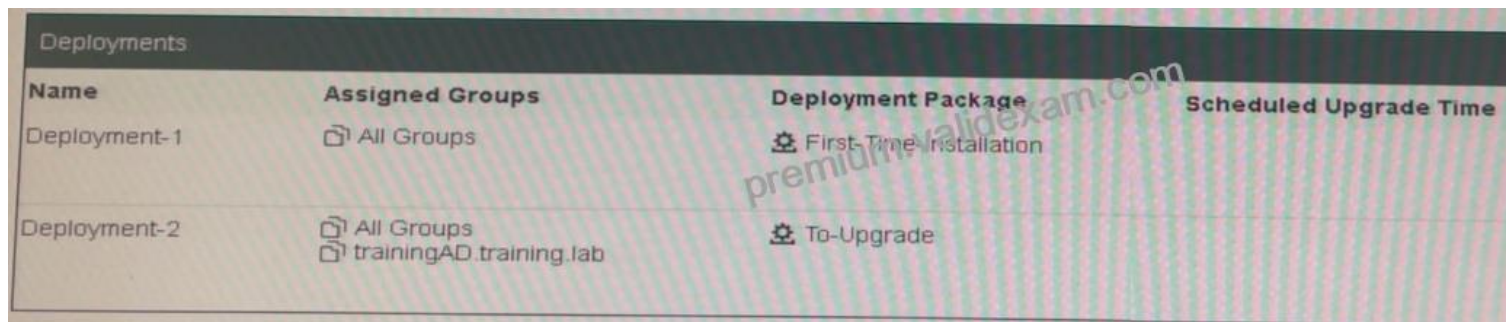
Q27. Refer to the exhibit.



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

- * FortiClient quarantines infected files and reviews later, after scanning them.
- * FortiClient blocks and deletes infected files after scanning them.
- * FortiClient scans infected files when the user copies files to the Resources folder
- * FortiClient copies infected files to the Resources folder without scanning them.

Q28. Refer to the exhibit.



Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time
Deployment-1	All Groups	First Time Installation	
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade	

Which shows FortiClient EMS deployment profiles.

When an administrator creates a deployment profile on FortiClient EMS, which statement about the deployment profile is true?

- * Deployment-1 will install FortiClient on new AD group endpoints
- * Deployment-2 will install FortiClient on both the AD group and workgroup
- * Deployment-2 will upgrade FortiClient on both the AD group and workgroup
- * Deployment-1 will upgrade FortiClient only on the workgroup

Q29. In a FortiSandbox integration, what does the remediation option do?

- * Wait for FortiSandbox results before allowing files
- * Exclude specified files
- * Alert and notify only
- * Deny access to a file when it sees no results

Q30. Which two statements are true about ZTNA? (Choose two.)

- * ZTNA provides role-based access
- * ZTNA manages access for remote users only
- * ZTNA manages access through the client only
- * ZTNA provides a security posture check

Q31. Refer to the exhibit.

```
eventtime=1633084101662546935 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=100.64.2.253 srcport=58664 srcintf="port1"
srcintfrole="wan" dstip=100.64.1.10 dstport=9443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=5215 proto=6 action="deny" policyid=0
policytype="proxy-policy" service="tcp/9443"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: failed to match a proxy-policy"
utmref=65462-14
```


Which shows the output of the ZTNA traffic log on FortiGate.

What can you conclude from the log message?

- * The remote user connection does not match the explicit proxy policy.
- * The remote user connection does not match the ZTNA server configuration.
- * The remote user connection does not match the ZTNA rule configuration.
- * The remote user connection does not match the ZTNA firewall policy

Accurate & Verified Answers As Seen in the Real Exam here: https://www.validexam.com/NSE5_FCT-7.0-latest-dumps.html