Fortinet.FCP_FCT_AD-7.4.v2026-08-31.q61

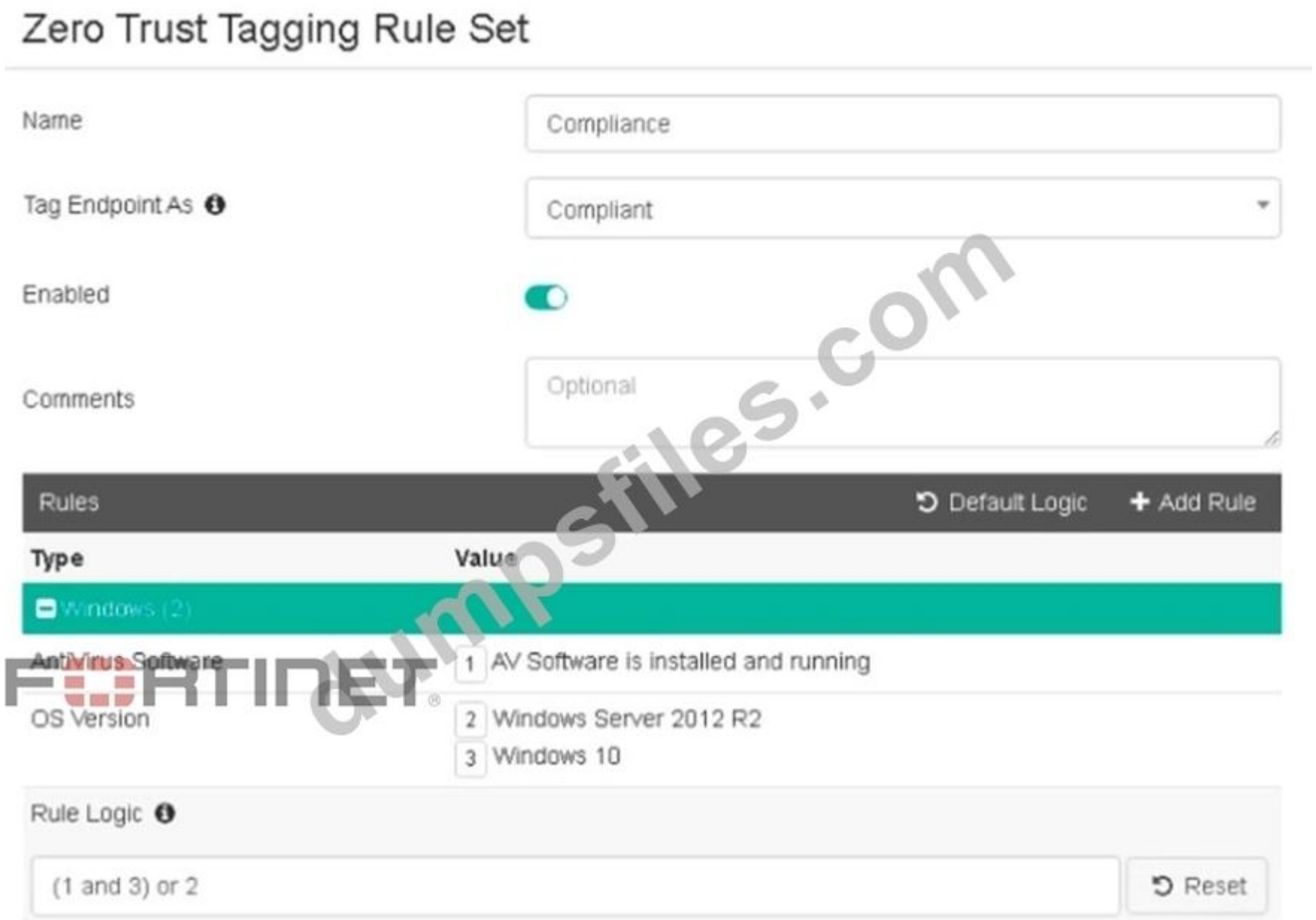
Exam Code:	FCP_FCT_AD-7.4
Exam Name:	FCP - FortiClient EMS 7.4 Administrator
Certification Provider:	Fortinet
Free Question Number:	61
Version:	v2026-08-31
# of views:	679
# of Questions views:	750
https://www.dumpsfiles.com/files/Fortinet/FCP_FCT_AD-7.4/Fortinet.FCP_FCT_AD-7.4.v2026-08-31.q61	

NEW QUESTION: 1
Which component or device shares device status information through ZTNA telemetry?
A. FortiClient
B. FortiGate
C. FortiGate Access Proxy
D. FortiClient EMS
Answer: A (LEAVE A REPLY)
FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

NEW QUESTION: 2
Which two statements are true about the ZTNA rule? (Choose two.)
A. It applies security profiles to protect traffic
B. It applies SNAT to protect traffic.
C. It defines the access proxy.
D. It enforces access control.
Answer: (SHOW ANSWER)
* Understanding ZTNA Rule Configuration:
* The ZTNA rule configuration shown in the exhibit defines how traffic is managed and controlled based on specific tags and conditions.
* Evaluating Rule Components:
* The rule includes security profiles to protect traffic by applying various security checks (A).
* The rule also enforces access control by determining which endpoints can access the specified resources based on the ZTNA tag (D).
* Eliminating Incorrect Options:
* SNAT (Source Network Address Translation) is not mentioned as part of this ZTNA rule.
* The rule does not define the access proxy but uses it to enforce access control.
* Conclusion:
* The correct statements about the ZTNA rule are that it applies security profiles to protect traffic (A) and enforces access control (D).
References:

ZTNA rule configuration documentation from the study guides.

NEW QUESTION: 3
Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.



Which two statements about the rule set are true? (Choose two.)
A. The endpoint must satisfy that only Windows 10 is running.
B. The endpoint must satisfy that only AV software is installed and running.
C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.
D. The endpoint must satisfy that only Windows Server 2012 R2 is running.
Answer: C,D (LEAVE A REPLY)
Based on the Zero Trust Tagging Rule Set configuration shown in the exhibit:
The rule set includes two conditions:
AV Software is installed and running
OS Version is Windows Server 2012 R2 or Windows 10

The Rule Logic is specified as "(1 and 3) or 2," meaning:
The endpoint must have antivirus software installed and running and must be running Windows 10.
Alternatively, the endpoint must be running Windows Server 2012 R2.
Therefore, the endpoint must satisfy either:
Antivirus is installed and running and Windows 10 is running.
Windows Server 2012 R2 is running.

NEW QUESTION: 4
Refer to the exhibit.

Based on The settings shown in The exhibit, which statement about FortiClient behaviour is Hue?
A. FortiClient scans infected files when the user copies files to the Resources folder.
B. FortiClient quarantines infected ties and reviews later, after scanning them.
C. FortiClient copies infected files to the Resources folder without scanning them.
D. FortiClient blocks and deletes infected files after scanning them.
Answer: A (LEAVE A REPLY)
Based on the settings shown in the exhibit, FortiClient is configured to scan files as they are downloaded or copied to the system. This means that if a user copies files to the "Resources" folder, which is not listed under exclusions, FortiClient will scan these files for infections. The exclusion path mentioned in the settings, "C:\Users\Administrator\Desktop\Resources", indicates that any files copied to this specific folder will not be scanned, but since the question implies that the "Resources" folder is not the same as the excluded path, FortiClient will indeed scan the files for infections.

NEW QUESTION: 5
Which two statements are true about ZTNA? {Choose two.)
A. ZTNA manages access for remote users only.
B. ZTNA provides role-based access.
C. ZTNA provides a security posture check.
D. ZTNA manages access through the client only.

Answer: (SHOW ANSWER)
ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.
Two functions of ZTNA are:
ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.
ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

NEW QUESTION: 6
FortiGate devices in the Security Fabric must receive endpoint from the FortiClient EMS for policy enforcement. Which is required to synchronize endpoint information?
A. FortiGate devices must function as gateway devices for the endpoints to receive endpoint information.
B. FortiGate devices must be authorized on the FortiClient EMS to receive endpoint information.
C. FortiGate devices must have the endpoint license.
D. FortiGate devices must run the same firmware version as FortiClient EMS.
Answer: (SHOW ANSWER)
FortiGate devices in the Security Fabric must securely connect and be authorized by the FortiClient EMS to synchronize endpoint and Security Posture tag information. This connection requires establishing a trusted certificate chain to the EMS server and authorizing the FortiGate on the EMS. Once authorized, the FortiGate can pull endpoint information such as dynamic tags from the EMS for policy enforcement.

NEW QUESTION: 7
Which component or device defines ZTNA lag information in the Security Fabric integration?
A. FortiClient
B. FortiGate
C. FortiClient EMS
D. FortiGate Access Proxy
Answer: C (LEAVE A REPLY)
* Understanding ZTNA:
* Zero Trust Network Access (ZTNA) requires defining tags for identifying and managing endpoint access.
* Evaluating Components:
* FortiClient EMS is responsible for managing and defining ZTNA tag information within the Security Fabric.
* Conclusion:
* The correct component that defines ZTNA tag information in the Security Fabric integration is FortiClient EMS.
References:
ZTNA and FortiClient EMS configuration documentation from the study guides.

NEW QUESTION: 8
An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient. What must the administrator do to achieve this requirement?
A. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
B. Disable select the vulnerability scan feature in the deployment package

C. Click the hide icon on the vulnerability scan profile assigned to endpoint
D. Use the default endpoint profile
Answer: C (LEAVE A REPLY)
Requirement Analysis:
The administrator needs to maintain a software vulnerability scan on endpoints without showing the feature on FortiClient.
Evaluating Options:
Disabling the feature in the deployment package or endpoint profile would remove the functionality entirely, which is not desired.
Using the default endpoint profile may not meet the specific requirement of hiding the feature.
Clicking the hide icon on the vulnerability scan profile assigned to the endpoint will keep the feature active but hidden from the user's view.
Conclusion:
The correct action is to click the hide icon on the vulnerability scan profile assigned to the endpoint (C).

NEW QUESTION: 9
What does FortiClient do as a fabric agent? (Choose two.)
A. Provides IOC verdicts
B. Creates dynamic policies
C. Provides application inventory
D. Automates Responses
Answer: (SHOW ANSWER)
Forticlient can also automate process of quarantine suspicious or compromised hosts.

NEW QUESTION: 10
Which statement about the FortiClient enterprise management server is true?
A. It receives the CA certificate from FortiGate to validate client certrficates.
B. It provides centralized management of multiple endpoints running FortiClient software.
C. It receives the configuration information of endpoints from ForuGate.
D. It enforces compliance on the endpoints using tags
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
In a ForliSandbox integration, what does the remediation option do?
A. Deny access to a tile when it sees no results
B. Alert and notify only
C. Exclude specified files
D. Wait for FortiSandbox results before allowing files
Answer: B (LEAVE A REPLY)
* Understanding FortiSandbox Integration:
* In a FortiSandbox integration, various remediation options are available for handling suspicious files.
* Evaluating Remediation Options:
* The remediation option for alerting and notifying without blocking access or waiting for results is essential to understand.
* Conclusion:

* The correct action for the remediation option in this context is to alert and notify only.
References:
FortiSandbox integration documentation from the study guides.

NEW QUESTION: 12
Refer to the exhibits. 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)?

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

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.
Answer: (SHOW ANSWER)
Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:
Enable Remote HTTPS Access to EMS: This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate.
Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

NEW QUESTION: 13
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
```

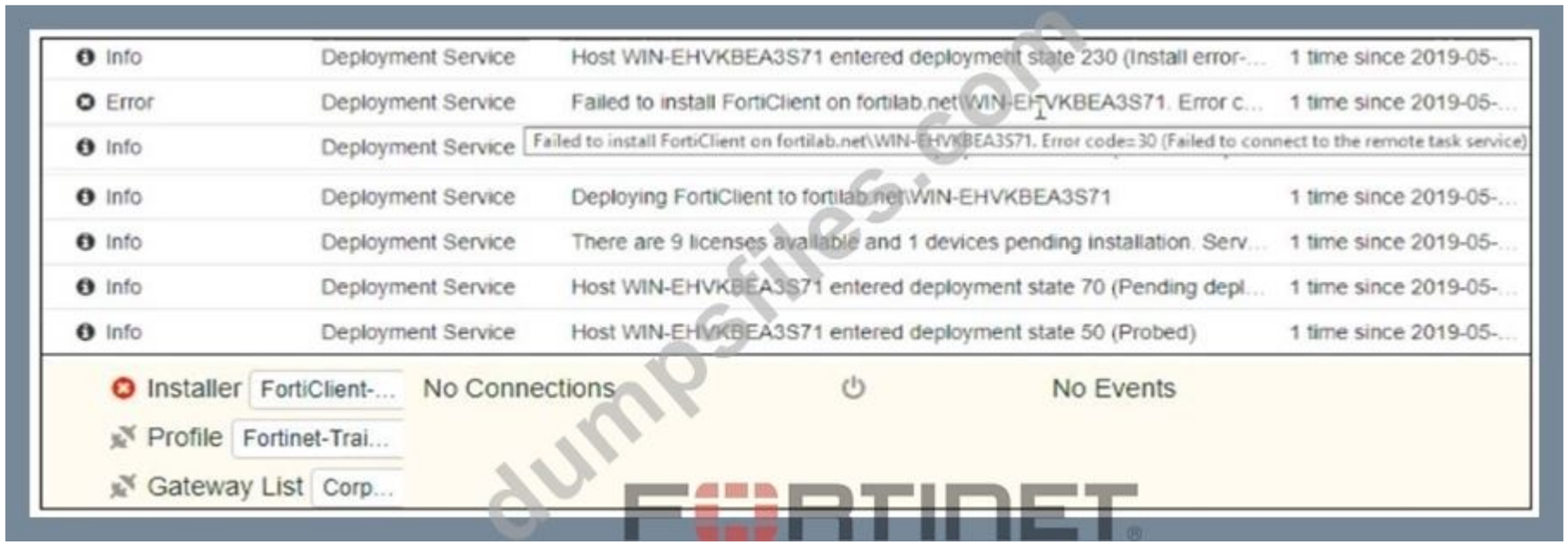
Based on the FortiClient logs shown in the exhibit which application is blocked by the application firewall?
A. Twitter
B. Facebook

C. Internet Explorer
D. Firefox
Answer: D (LEAVE A REPLY)
Based on the FortiClient logs shown in the exhibit:
* The first log entry shows the application "firefox.exe" trying to access a destination IP, with the threat identified as "Twitter."
* The action taken by the application firewall is "blocked" with the event type "appfirewall." This indicates that the application firewall has blocked access to Twitter.
References
* FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section
* Fortinet Documentation on Interpreting FortiClient Logs

NEW QUESTION: 14
Which statement about deploying FortiClient EMS in an air-gapped environment is true?
A. You can generate FortiClient installers on the FortiClient EMS instance.
B. You can sync a license on the FortiClient EMS GUI using your FortiCloud account.
C. You can configure FortiClient EMS to receive updates from FortiManager.
D. You can use offline antimalware data on FortiClient EMS to operate in an air-gapped deployment.
Answer: (SHOW ANSWER)
In an air-gapped environment, FortiClient EMS cannot access the internet for updates. Using offline antimalware data allows FortiClient EMS to provide endpoint protection and operate without internet connectivity.

NEW QUESTION: 15
An administrator has a requirement to add user authentication to the ZTNA access for remote or off-fabric users Which FortiGate feature is required m addition to ZTNA?
A. FortiGate FSSO
B. FortiGate certificates
C. C. FortiGate explicit proxy
D. FortiGate endpoint control
Answer: (SHOW ANSWER)
For adding user authentication to the ZTNA access for remote or off-fabric users, the following FortiGate feature is required in addition to ZTNA:
* FortiGate explicit proxyallows FortiGate to intercept web traffic for authentication purposes.
* ZTNA integrates with various FortiGate features to provide secure access and ensure that users are authenticated before accessing resources.
* By using an explicit proxy, FortiGate can handle web traffic and enforce authentication policies for remote users who are not directly on the corporate network (off-fabric).
Thus, the correct feature to use for this requirement is the FortiGate explicit proxy.
References
* FortiGate Security 7.2 Study Guide, ZTNA and Proxy Configuration Sections
* Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW QUESTION: 16
Based on the logs shown in the exhibit, why did FortiClient EMS fail to install FortiClient on the endpoint?



A. The FortiClient antivirus service is not running.

B. The Windows installer service is not running.

C. The remote registry service is not running.

D. The task scheduler service is not running.

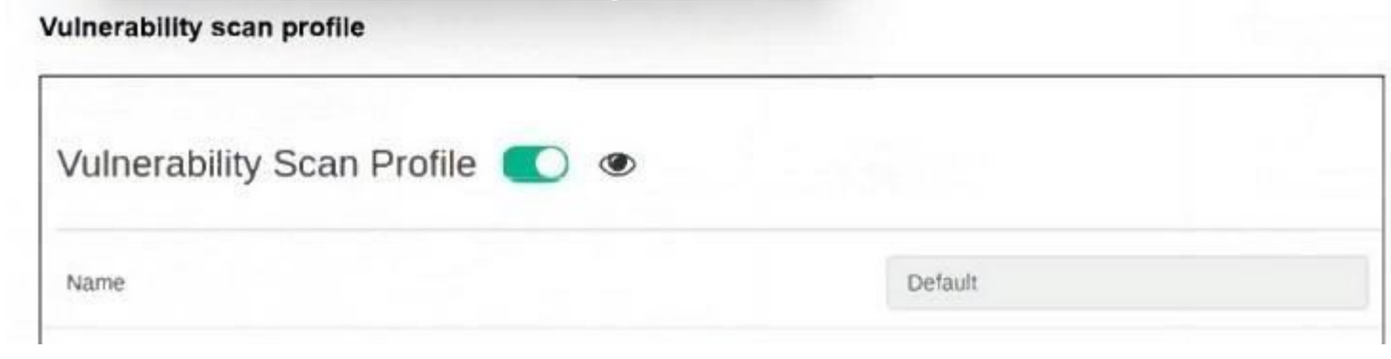
Answer: (SHOW ANSWER)

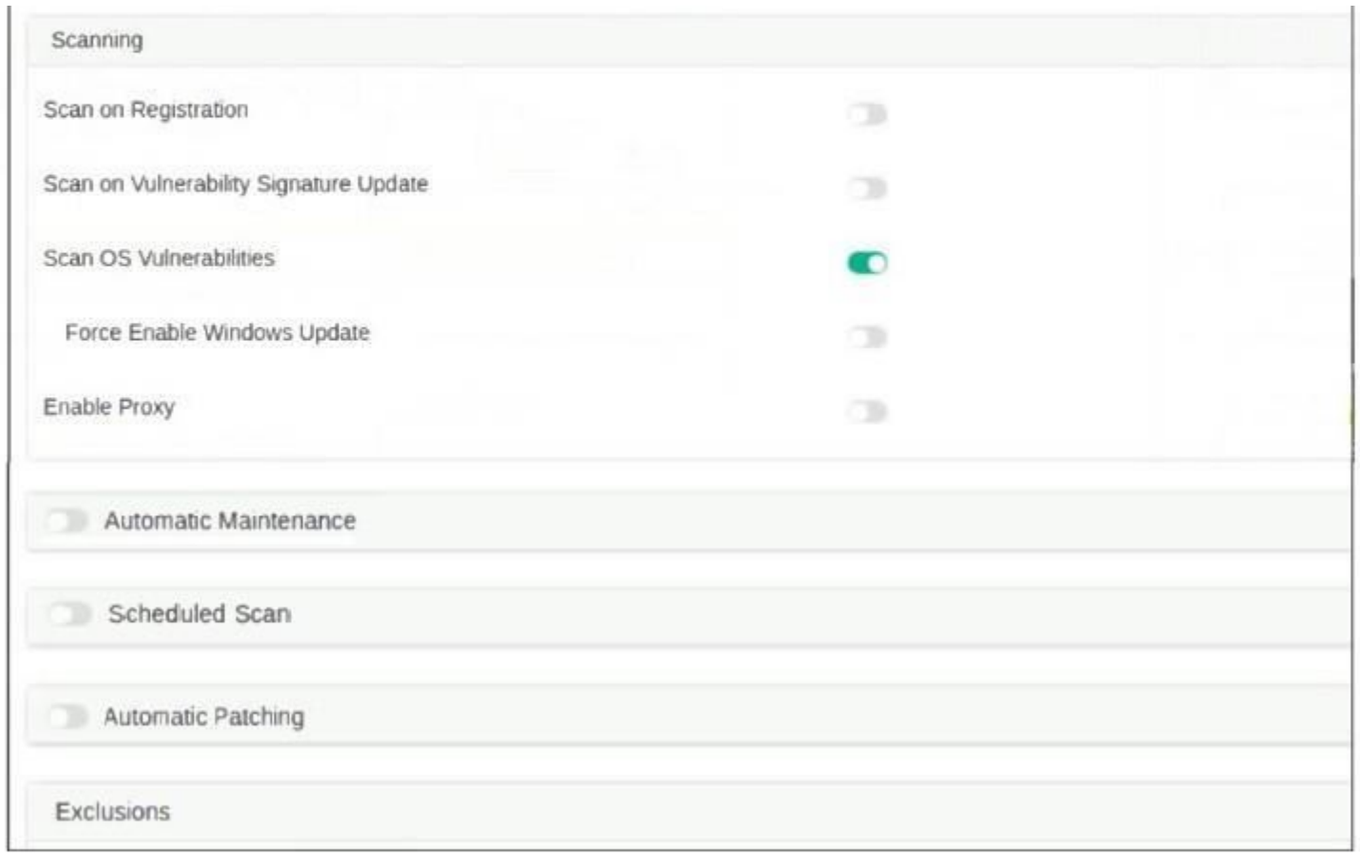
The deployment service error message may be caused by any of the following. Try eliminating them all, one at a time.

1. Wrong username or password in the EMS profile
2. Endpoint is unreachable over the network
3. Task Scheduler service is not running
4. Remote Registry service is not running
5. Windows firewall is blocking connection

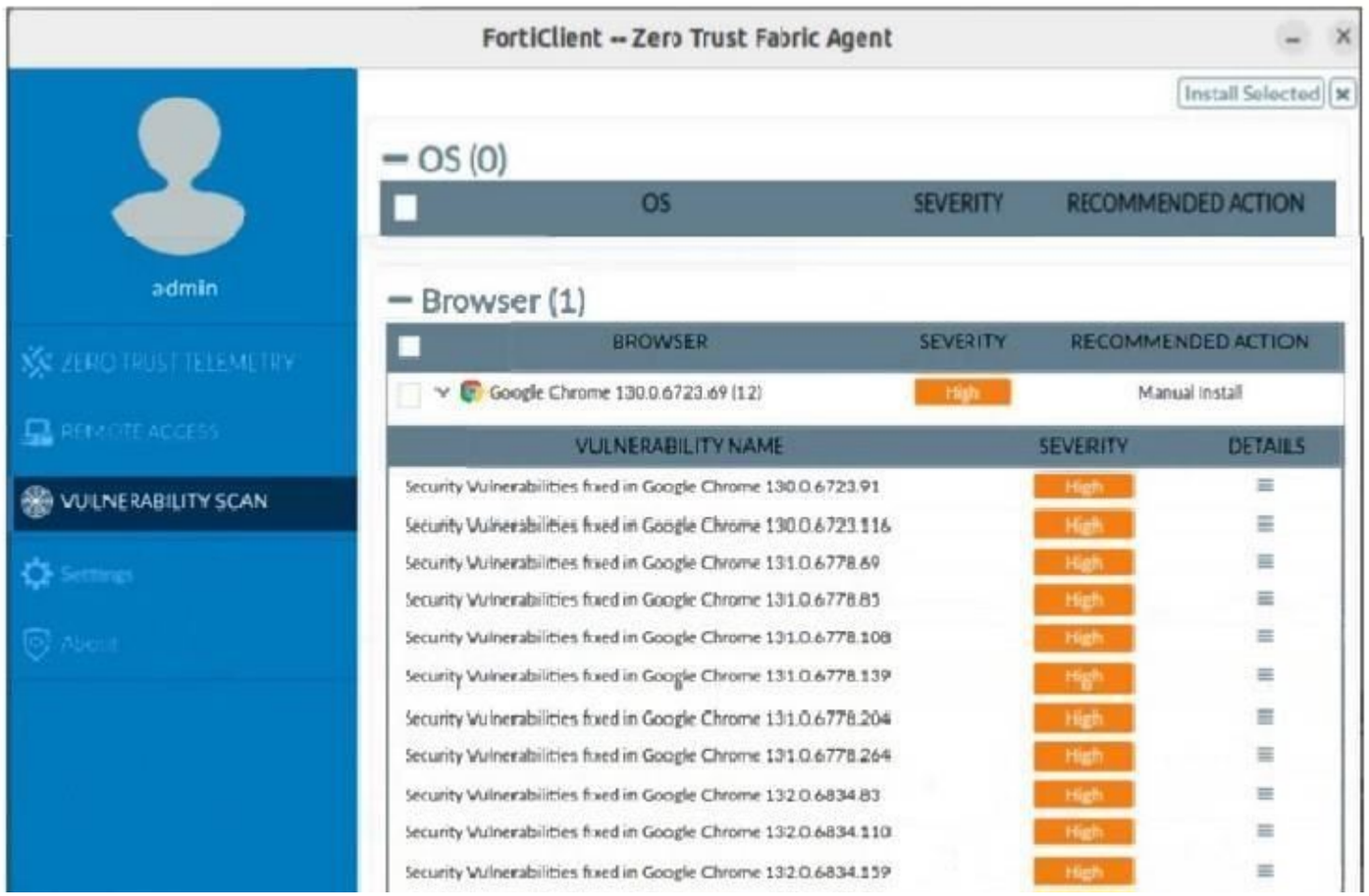
NEW QUESTION: 17

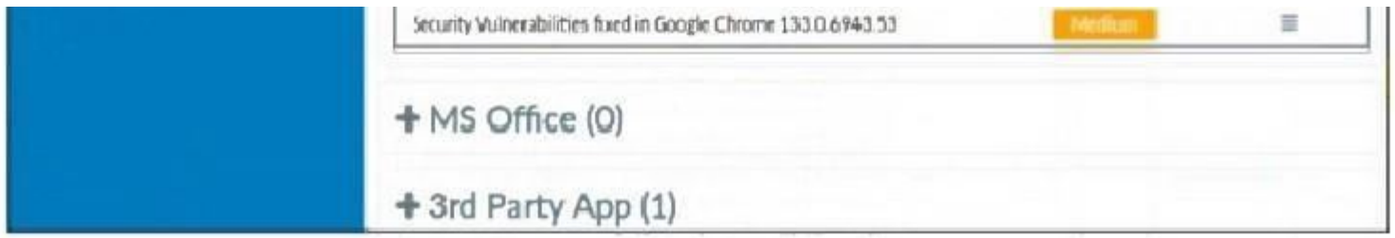
Refer to the exhibits. How will the vulnerability shown in the scan be patched?





FortiClient vulnerability scan





A. An administrator will patch the vulnerability remotely using FortiClient EMS.
B. The end user will patch the vulnerability by installing the patch from the vendors website.
C. The end user will patch the vulnerability using the FortiClient software.
D. The vulnerability will be patched automatically based on the endpoint profile configuration.
Answer: B (LEAVE A REPLY)
The vulnerability scan shows that the recommended action is "Manual Install," indicating that the end user must patch the vulnerability by manually downloading and installing the update from the vendor's website.

NEW QUESTION: 18
Refer to the exhibit. FortiGate has lost connectivity with FortiClient EMS.
What is causing this problem?

Output of fcnacd debugs

```
# diagnose debug application fcnacd -1
# diagnose debug enable

[ec_ez_worker_base_prep_resolver:381] Outgoing interface index 0 for 1 (ems).
[ec_ez_worker_base_prep_ssl:428] verify peer method: 3, current ssl_cb: (nil), new ssl_cb: 0x55abb196ced0
[ec_ems_context_submit_work:641] Call submitted successfully.
obj-id: 0, desc: REST API to get EMS Serial Number., entry: api/v1/system/serial_number.
[__match_server_cert_key:462] verify_peer_method: 3
[__match_server_cert_key:480] EMS CN does not match verified CN!
[__match_server_cert_key:519] ret=0
[ec_ez_worker_process:400] Processing call for obj-id: 0, entry: "api/v1/system/serial_number"
[_update_obj_stats:365] Storing (0, ems, 7)
[ec_ez_worker_process:458] Call completed with failure.
obj-id: 0, desc: "REST API to get EMS Serial Number.", entry: "api/v1/system/serial_number".
error info: Error (-1@__generic_process_result_ex:148). EMS verification data has changed on host or peer. Must reverify.
[ec_ez_worker_base_prep_resolver:381] Outgoing interface index 0 for 1 (ems).
[ec_ez_worker_base_prep_ssl:428] verify peer method: 3, current ssl_cb: (nil), new ssl_cb: 0x55abb196ced0
[ec_ems_context_submit_work:641] Call submitted successfully.
obj-id: 0, desc: REST API to get EMS Serial Number., entry: api/v1/system/serial_number.
[__match_server_cert_key:462] verify_peer_method: 3
```


A. FortiGate is not able to reach the IP address or FQDN of the FortiClient EMS server.
B. FortiGate is not able to verify the FortiClient EMS serial number.
C. FortiGate is not able to establish trust using the FortiClient EMS CA certificate.

D. FortiGate is not able to reach FortiClient EMS on telemetry port 8013.

Answer: B (LEAVE A REPLY)

The debug output shows "EMS verification data has changed on host or peer. Must reverify," indicating that FortiGate cannot verify the FortiClient EMS serial number, causing the connectivity issue.

NEW QUESTION: 19

In a FortiClient EMS deployment, what is the primary security function of the endpoint control certificate?

A. It is used to encrypt the telemetry connection from FortiClient to FortiClient EMS.

B. It is used by FortiClient Web Filter extension to perform SSL inspection on web traffic.

C. It is used to secure communication with FortiGate as part of the Security Fabric.

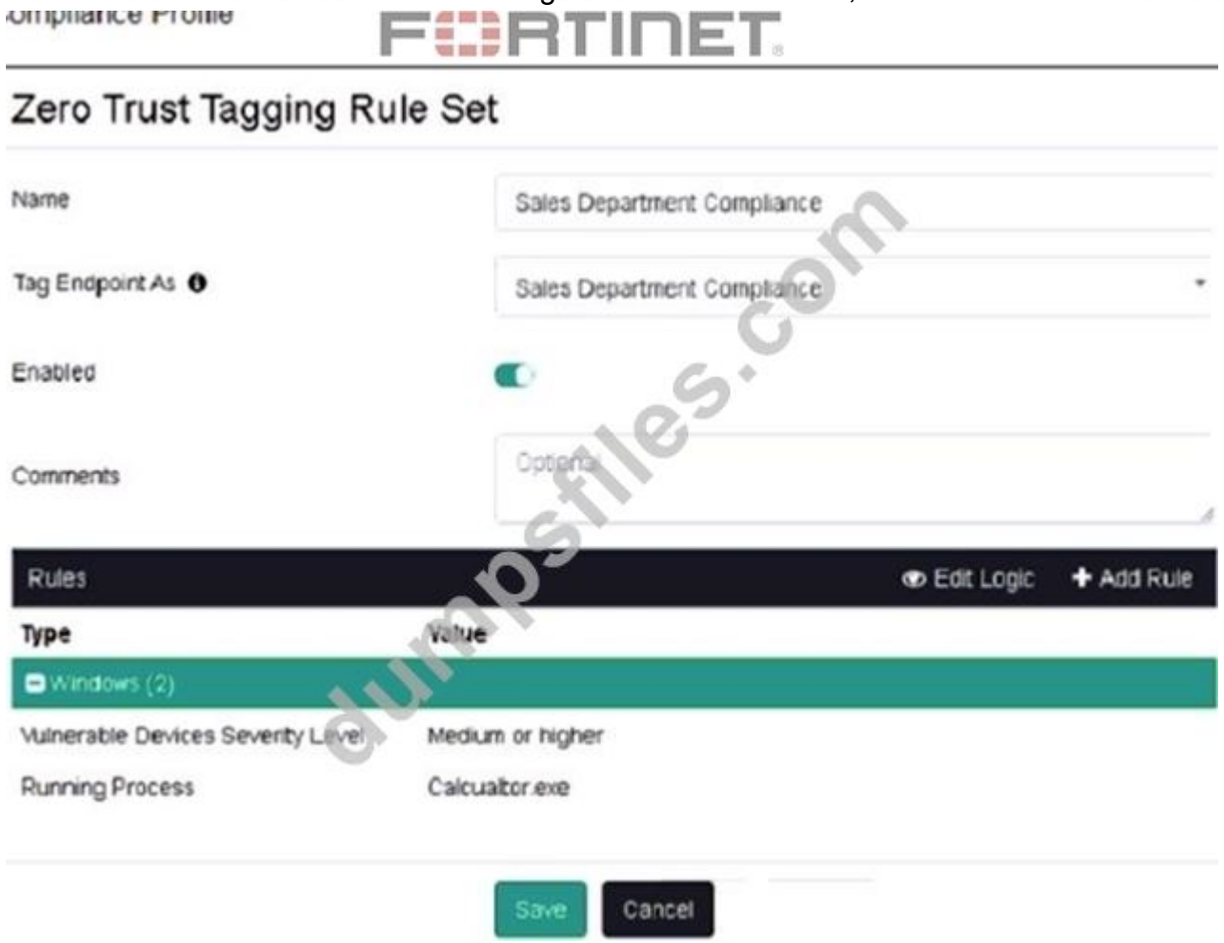
D. It is used to sign certificate requests from endpoints for zero trust network access (ZTNA).

Answer: D (LEAVE A REPLY)

The endpoint control certificate is used to sign certificate requests from FortiClient endpoints for ZTNA, enabling secure identity verification and establishing trust between endpoints and FortiClient EMS.

NEW QUESTION: 20

Refer to the exhibit. Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)



A. Enable the web filter profile.

B. Run Calculator application on the endpoint.

C. Integrate FortiSandbox tor infected file analysis

D. Patch applications that have vulnerability rated as high or above.

Answer: (SHOW ANSWER)

Observation of Compliance Profile:

The compliance profile shown in the exhibit includes rules for vulnerability severity level and running process (Calculator.exe).

Evaluating Actions for Compliance:

To make the endpoint compliant, the administrator needs to ensure that the vulnerability severity level is medium or higher is patched (D). Additionally, the Calculator.exe application must be running on the endpoint (B).

Eliminating Incorrect Options:

Enabling the web filter profile (A) is not related to the compliance rules shown.

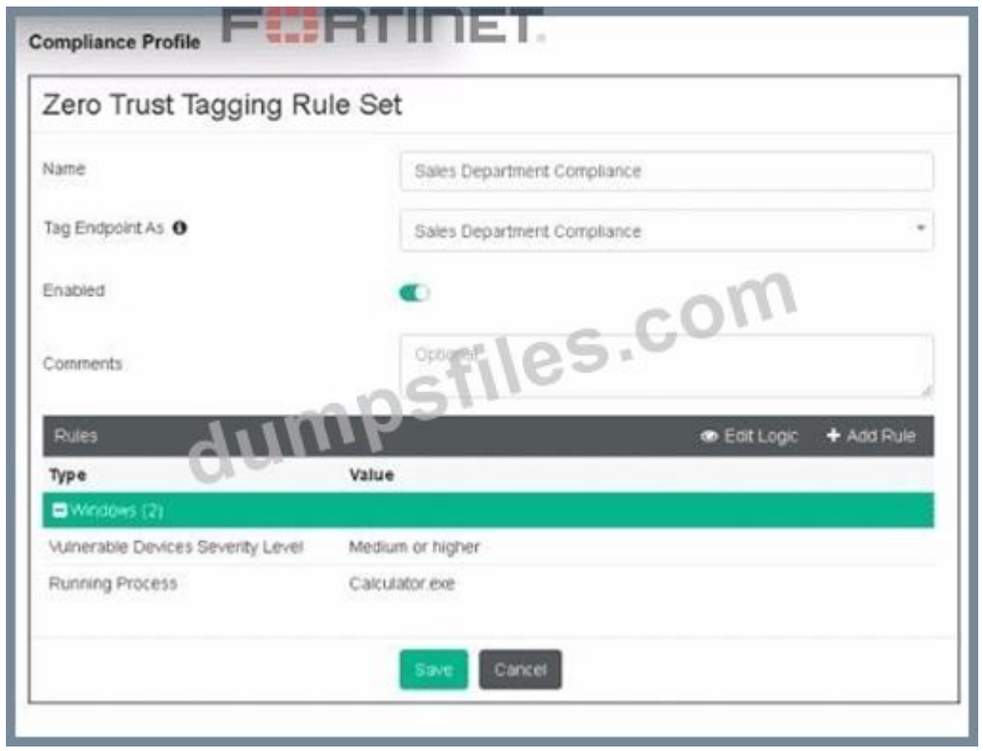
Integrating FortiSandbox (C) is not a requirement in the given compliance profile.

Conclusion:

The correct actions are to run the Calculator application on the endpoint (B) and patch applications with vulnerabilities rated as high or above (D).

NEW QUESTION: 21

Refer to the exhibit.



Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

A. Enable the web filter profile.

B. Run Calculator application on the endpoint.

C. Integrate FortiSandbox tor infected file analysis

D. Patch applications that have vulnerability rated as high or above.

Answer: (SHOW ANSWER)

* Observation of Compliance Profile:
* The compliance profile shown in the exhibit includes rules for vulnerability severity level and running process (Calculator.exe).
* Evaluating Actions for Compliance:
* To make the endpoint compliant, the administrator needs to ensure that the vulnerability severity level is medium or higher is patched (D).
* Additionally, the Calculator.exe application must be running on the endpoint (B).

* Eliminating Incorrect Options:
* Enabling the web filter profile (A) is not related to the compliance rules shown.
* Integrating FortiSandbox (C) is not a requirement in the given compliance profile.
* Conclusion:
* The correct actions are to run the Calculator application on the endpoint (B) and patch applications with vulnerabilities rated as high or above (D).
References:
FortiClient EMS compliance profile configuration documentation from the study guides.

NEW QUESTION: 22
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.
What could have caused this problem?
A. The FortiClient exe file is included in the distribution package
B. The FortiClient MST file is missing from the distribution package
C. FortiClient does not have permission to access the distribution package.
D. The FortiClient package is not assigned to the group
Answer: (SHOW ANSWER)
When deploying FortiClient via Microsoft AD Group Policy, it is essential to ensure that the deployment package is correctly assigned to the target group. The absence of custom configuration after installation can be due to several reasons, but the most likely cause is:
Deployment Package Assignment: The FortiClient package must be assigned to the appropriate group in Group Policy Management. If this step is missed, the installation may proceed, but the custom configurations will not be applied.
Thus, the administrator must ensure that the FortiClient package is correctly assigned to the group to include all custom configurations.

NEW QUESTION: 23
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
Answer: (SHOW ANSWER)
Understanding Compliance Rules:
The compliance rule for the sales department needs to be enforced dynamically.
Enforcing Compliance:
FortiGate is responsible for enforcing compliance by integrating with FortiClient EMS to apply dynamic access control based on compliance status.
Conclusion:
The Fortinet device that will enforce compliance with dynamic access control is the FortiGate.

NEW QUESTION: 24
Which security attribute is verified during the SSL connection negotiation between FortiClient and FortiClient EMS to mitigate man-in-the-middle (MITM) attacks? (Choose one answer)
A. serial number (SN)
B. common name (CN)

C. location (L)
D. organization (O)
Answer: B (LEAVE A REPLY)
According to theFortiClient EMS Administrator Study Guide (7.2/7.4 versions)and theFortinet Document LibraryregardingSSL/TLS Endpoint Communication Security, the primary attribute verified during the SSL connection negotiation to mitigate Man-in-the-Middle (MITM) attacks is theCommon Name (CN).
1. SSL Connection Negotiation & MITM Mitigation
* Verification Process: When FortiClient attempts to establish aTelemetry connectionwith the FortiClient EMS server, an SSL handshake occurs. To ensure it is communicating with the legitimate server and not a malicious interceptor (MITM), FortiClient verifies the server's certificate.
* Role of the Common Name (CN): TheCommon Name(or theSubject Alternative Name - SAN) in the certificate must match theFQDN (Fully Qualified Domain Name)or theIP addressthat the client intended to connect to.
* Security Enforcement: If the CN/SAN does not match the server's expected address, FortiClient will detect a discrepancy. Depending on theInvalid Certificate Actionsetting in the profile (e.g., Warn or Block), it will prevent the establishment of a secure session to stop the MITM attacker from masquerading as the EMS server.
2. Why Other Options are Incorrect/Secondary
* A. Serial Number (SN): While every certificate has a unique Serial Number, it is primarily used by the Certificate Authority (CA) for tracking and revocation purposes. While FortiOS 7.2.4+ can use SN for certain restricted VPN checks, the core SSL negotiation mechanism for identifying a specific host to prevent spoofing relies on theCN/SANfields.
* C. Location (L) and D. Organization (O): These are descriptive fields within the certificate'sSubject that provide geographical and corporate information. They are not functionally used by the SSL/TLS protocol to verify the identity of the host during the connection negotiation or to mitigate MITM attacks.
3. Curriculum References
* EMS Administration Guide (System Settings Profile): Details how the client verifies the EMS server certificate. It specifies that for a connection to be trusted, the server address must align with the certificate's identity fields (CN/SAN).
* FortiGate/FortiOS 7.2.4 New Features: Highlights the specific enhancement where FortiClient EMS connectors now "trust EMS server certificate renewals based on theCN field" to ensure continuous secure communication.

NEW QUESTION: 25
An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate What is the prerequisite to get FortiClient EMS lo connect to FortiGate successfully?
A. Import and verify the FortiClient EMS tool CA certificate on FortiGate.
B. Revoke and update the FortiClient client certificate on EMS.
C. Import and verify the FortiClient client certificate on FortiGate.
D. Revoke and update the FortiClient EMS root CA.
Answer: (SHOW ANSWER)
Connecting FortiClient EMS to FortiGate:
The administrator needs to establish a connection between FortiClient EMS and FortiGate as a fabric connector.
Prerequisites for Connection:
A key prerequisite is the import and verification of the FortiClient EMS tool CA certificate on FortiGate to ensure a trusted connection.
Conclusion:
The correct prerequisite for a successful connection is to import and verify the FortiClient EMS tool CA certificate on FortiGate.

NEW QUESTION: 26
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   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 lo the ForliClient endpoint from the EMS server?

A. Fortinet-Training

B. Default configuration policy c

C. Compliance rules default

D. Default

Answer: (SHOW ANSWER)

* Observation of Logs:

* The logs show a policy named "Fortinet-Training" being applied to the endpoint.

* Evaluating Policies:

* The log entries indicate that the "Fortinet-Training" policy was received and applied.

* Conclusion:

* Based on the logs, the currently applied policy on the FortiClient endpoint is "Fortinet-Training".

References:

FortiClient EMS policy configuration and log analysis documentation from the study guides.

NEW QUESTION: 27

Which Fortinet solution can you integrate FortiClient with to use the single sign-on mobility agent (SSOMA) feature? (Choose one answer)

A. FortiAuthenticator

B. FortiSASE

C. FortiPAM

D. FortiNAC

Answer: (SHOW ANSWER)

According to theFortiClient EMS 7.2/7.4 Administration GuideandFortiAuthenticator Study Guides, the Single Sign-On Mobility Agent (SSOMA)is a feature specifically designed to integrate with FortiAuthenticatorto provide transparent, identity-based authentication.

1. Integration with FortiAuthenticator (Answer A)

* The SSOMA Service:The mobility agent service is hosted on theFortiAuthenticatorunit.

Administrators must navigate toFortinet SSO Methods > SSO > Generalon the FortiAuthenticator and toggle onEnable FortiClient SSO Mobility Agent Service.

* Communication Protocol:FortiClient communicates with FortiAuthenticator via a specified TCP listening port (defaulting to8001or8005) and uses apre-shared key(secret key) for authentication.

* Transparent Authentication:Once configured, the SSOMA on the endpoint automatically sends user logon information and IP address changes (such as WiFi roaming)

to FortiAuthenticator.
FortiAuthenticator then shares this information with FortiGate units to enforce identity-based security policies without the user needing to re-authenticate manually.
2. Modern Capabilities (Azure AD / Entra ID)
* Cloud Integration:In FortiClient 7.2.1 and later, SSOMA supportsnative Azure AD (Entra ID). In this mode, the agent sends the Azure AD domain and tenant ID directly to FortiAuthenticator, allowing organizations to create identity-based policies for cloud-joined devices.
3. Note on FortiPAM (Option C)
* Recent Updates:While recent FortiClient EMS 7.4 documentation mentions an"Add FortiPAM agent to SSOMA"feature, this is an extension of the existing SSOMA framework. The core product that defines and runs the SSOMA service for general Single Sign-On (SSO) remainsFortiAuthenticator.
4. Why Other Options are Incorrect
* B. FortiSASE:While FortiSASE uses FortiClient for Secure Internet Access (SIA), it uses different mechanisms (like SAML or the SASE cloud portal) for user identity rather than the specific SSOMA agent service.
* D. FortiNAC:FortiNAC uses FortiClient for persistent agent-based posture assessment and scanning, but it does not utilize the SSOMA mobility agent for user-to-IP mapping.

NEW QUESTION: 28
Which statement about FortiClient enterprise management server is true?
A. It provides centralized management of multiple endpoints running FortiClient software.
B. It provides centralized management of FortiClient Android endpoints only.
C. It provides centralized management of FortiGate devices.
D. It provides centralized management of Chromebooks running real-time protection
Answer: A (LEAVE A REPLY)
FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

NEW QUESTION: 29
Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

When an administrator creates a deployment profile on FortiClient EMS.
Which statement about the deployment profile is true?
A. Deployment-2 will upgrade FortiClient on both the AD group and workgroup.
B. Deployment-1 will install FortiClient on new AO group endpoints.
C. Deployment-2 will install FortiClient on both the AD group and workgroup.
D. Deployment-1 will upgrade FortiClient only on the workgroup.
Answer: (SHOW ANSWER)
Deployment Profiles Analysis:
Deployment-1 has the "First-Time-Installation" package and is assigned to "All Groups" with a priority of 1 but is not enabled.

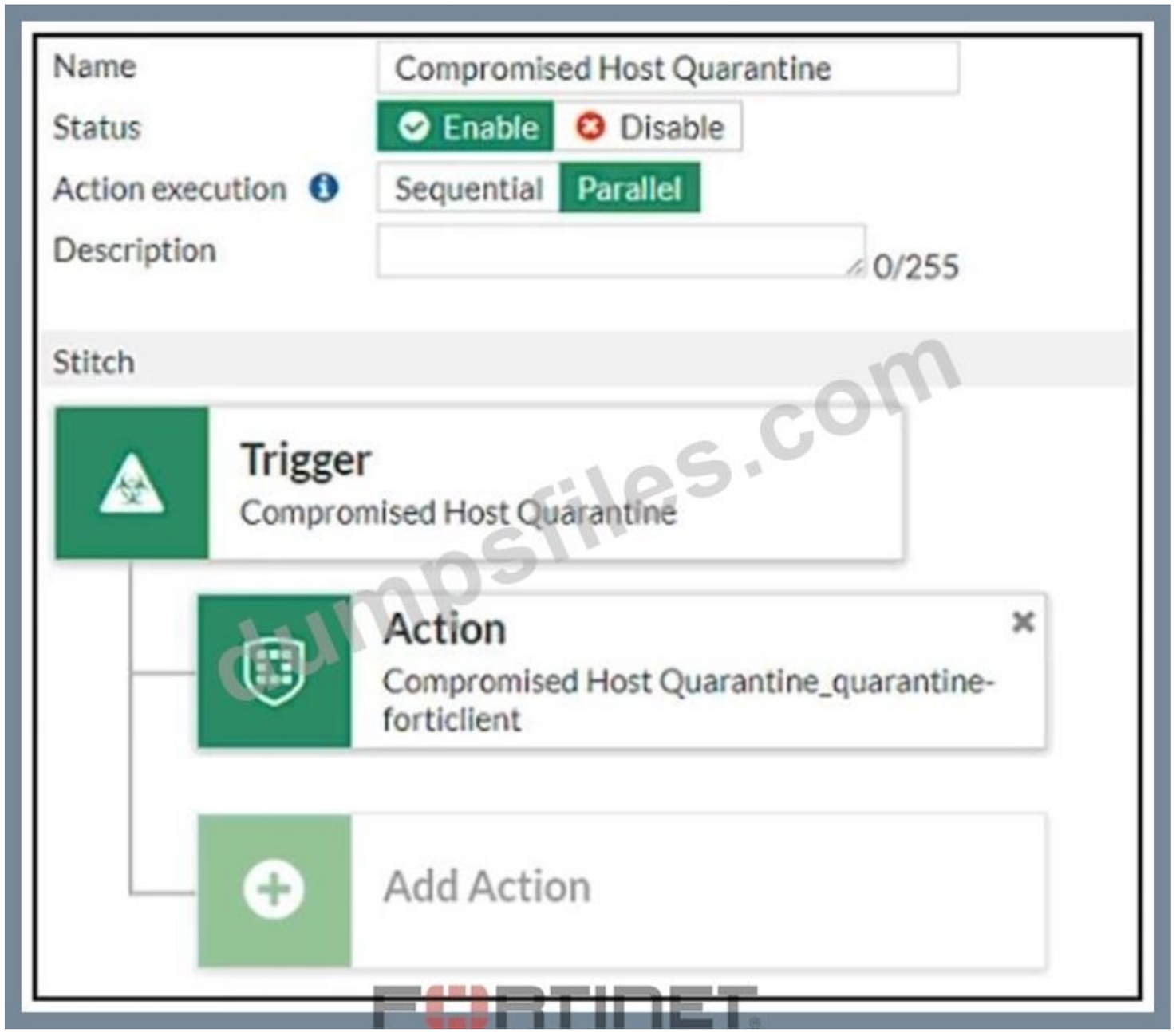
Deployment-2 has the "To-Upgrade" package, is assigned to both "All Groups" and "trainingAD.training.lab," with a priority of 2 and is enabled.
Evaluating Deployment-2:
Deployment-2 will upgrade FortiClient on both "All Groups" and "trainingAD.training.lab" since it is enabled and assigned to these groups. This includes both AD (Active Directory) groups and workgroups.
Conclusion:
Since Deployment-2 is set to upgrade FortiClient on all the assigned groups and workgroups, the correct answer is A.

NEW QUESTION: 30
Refer to the exhibit.

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
Answer: (SHOW ANSWER)
Block Malicious Website has nothing to do with infected files. Since Realtime Protection is OFF, it will be allowed without being scanned.
Based on the settings shown in the exhibit:
* Realtime Protection:OFF
* Dynamic Threat Detection:OFF
* Block malicious websites:ON
* Threats Detected:75
The "Realtime Protection" setting is crucial for preventing infected files from being downloaded and executed. Since "Realtime Protection" is OFF, FortiClient will not actively scan files being downloaded. The setting "Block malicious websites" is intended to prevent access to known malicious websites but does not scan files for infections.
Therefore, when a user tries to download an infected file, FortiClient will allow the file to download without scanning it due to the Realtime Protection being OFF.
References

* FortiClient EMS 7.2 Study Guide, Antivirus Protection Section
* Fortinet Documentation on FortiClient Real-time Protection Settings

NEW QUESTION: 31
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
Answer: (SHOW ANSWER)
Based on the Security Fabric automation settings shown in the exhibit:
The automation stitch is configured with a trigger for a "Compromised Host." The action specified for this trigger is "Quarantine FortiClient via EMS." This indicates that when an endpoint is detected as compromised, FortiClient EMS will quarantine the endpoint as part of the automation process.

Therefore, the action taken on compromised endpoints will be to quarantine them through EMS.

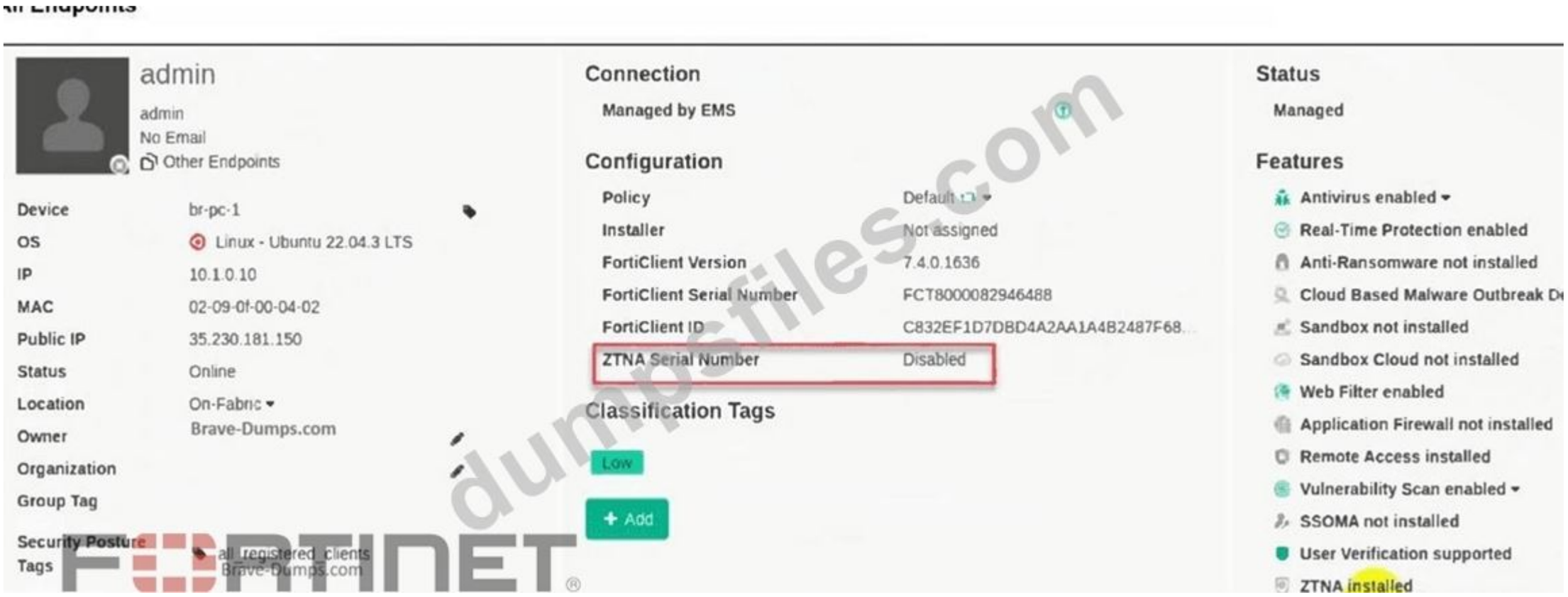
NEW QUESTION: 32
What does FortiClient do as a fabric agent? (Choose two.)
A. Provides application inventory
B. Creates dynamic policies
C. Provides IOC verdicts
D. Automates Responses
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 33
Which two statements about FortiClient EMS integration with Active Directory (AD) are true? (Choose two answers)
A. FortiClient EMS has full read-write access on the AD server.
B. FortiClient installations on domain endpoints can deployed from FortiClient EMS.
C. Endpoint profiles can be assigned to endpoints based on domain groups.
D. Imported AD endpoints cannot be directly deleted on FortiClient EMS
Answer: B,C (LEAVE A REPLY)
Based on theFortiClient EMS 7.2/7.4 Administration Guideand theEMS Administrator Study Guide, the integration with Active Directory (AD) provides several automated management capabilities.
1. Analysis of the True Statements:
* B. FortiClient installations on domain endpoints can be deployed from FortiClient EMS:
* FortiClient EMS allows administrators to createDeployment Profilesspecifically for Windows endpoints discovered via AD.
* By providingAD administrator credentialswithin the deployment profile, EMS can remotely push the FortiClient MSI installer to domain-joined endpoints that do not yet have the software installed.
* C. Endpoint profiles can be assigned to endpoints based on domain groups:
* The core benefit of AD integration is the ability to mapEndpoint Policiesto specificAD Organizational Units (OUs)orSecurity Groups.
* When an endpoint policy is assigned to an AD group, all FortiClient endpoints belonging to that group automatically receive the associated security profiles (Antivirus, Web Filter, VPN, etc.) defined within that policy.
2. Why Other Options are Incorrect/Secondary:
* A. FortiClient EMS has full read-write access on the AD server:
* The curriculum states explicitly that theLDAP/AD connection is read-only.
* EMS cannot modify AD objects, create users, or change group memberships; it only synchronized information from the AD server to the EMS database.
* D. Imported AD endpoints cannot be directly deleted on FortiClient EMS:
* While technically true in a functional sense (deleting a synced endpoint will result in it being re- added during the next sync unless it is removed from the AD OU), the

curriculum typically prioritizesB and Cas the primary functional "features" of the integration.
* Note that the guide specifies the "Delete" action in the Endpoints pane is restricted tonon- domain devicesto prevent synchronization conflicts.
3. Summary of Integration Features:
* Sync Schedule:EMS periodically syncs with AD (default every 10 minutes) to update the endpoint list.
* Policy Automation:Moving a user or computer to a different group in AD will cause EMS to automatically update their security posture based on the new group's assigned policy.

NEW QUESTION: 34
An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?
A. It redirects the client request to the access proxy.
B. It uses the access proxy.
C. It defines ZTNA server.
D. It only uses ZTNA tags to control access for endpoints.
Answer: A (LEAVE A REPLY)
The firewall policy matches and redirects client requests to the access proxy VIP.
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration

NEW QUESTION: 35
Refer to the exhibit.



The zero trust network access (ZTNA) serial number on endpoint br-pc-1 is in a disabled state.
What is causing the problem? (Choose one answer)
A. The ZTNA feature is not installed on FortiClient.
B. The ZTNA destinations endpoint profile is disabled.

C. The ZTNA is disabled due to FortiClient disconnected from FortiClient EMS.
D. The ZTNA certificate has been revoked by administrator.
Answer: B (LEAVE A REPLY)
Based on theFortiClient EMS 7.2/7.4 Study Guidesand the visual evidence provided in the exhibit, here is the verified breakdown of why theZTNA Serial Numberis showing asDisabled:
1. Analysis of the Exhibit
* Operating System:The endpoint is runningLinux (Ubuntu 22.04.3 LTS).
* Connection Status:The endpoint status isOnlineandManaged by EMS. This immediately eliminates Option C, as the device is actively communicating with the EMS server.
* Features List:At the bottom right of the "Features" column, it explicitly states"ZTNA installed". This eliminatesOption A, confirming the software component is present on the endpoint.
* ZTNA Serial Number Field:The field is highlighted in red and shows"Disabled".
2. Identifying the Root Cause (Option B)
In the FortiClient EMS curriculum regardingZTNA (Zero Trust Network Access), the ZTNA Serial Number (also known as the ZTNA Tagging or Client Certificate UID) is generated and activated based on the assigned Endpoint Profile.
* Profile Dependency:For FortiClient to generate a ZTNA serial number/certificate and participate in ZTNA, the administrator must enable and configure theZTNA Destinations(or ZTNA Connection) profile within the EMS.
* Disabled State:If theZTNA Destinationsfeature is disabled in the profile assigned to that specific endpoint (or if the endpoint is assigned the "Default" profile where ZTNA is not configured), the
"ZTNA Serial Number" status on the EMS dashboard will reflect asDisabled.
* Linux Specifics:In FortiClient for Linux, ZTNA support is available but requires the profile to be explicitly pushed and active. If the profile is toggled off in the EMS GUI underEndpoint Profiles > ZTNA Destinations, the serial number functionality is suspended.
3. Why Other Options are Incorrect
* A. The ZTNA feature is not installed:The exhibit clearly shows "ZTNA installed" under the Features list.
* C. FortiClient disconnected from EMS:The exhibit shows the status as "Online" and "Managed by EMS" with a green checkmark.
* D. The ZTNA certificate has been revoked:If a certificate is revoked, the status typically shows as
"Revoked" or "Expired," or the serial number would still be present but marked as untrusted. A
"Disabled" state indicates the feature itself is turned off at the policy/profile level.

NEW QUESTION: 36
An administrator must deploy FortiClient for an organization that has BYOD and remote users.
What can the administrator use to deploy FortiClient?
A. FortiClient zero-touch provisioning
B. Microsoft System Center Configuration Manager (SCCM)
C. Microsoft Intune
D. Group policy Object (GPO)
Answer: (SHOW ANSWER)
FortiClient zero-touch provisioning is specifically designed to deploy FortiClient to BYOD and remote users without requiring manual installation or corporate device management tools.

NEW QUESTION: 37

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

A. Proxy scan

B. Full scan

C. Custom scan

D. Flow scan

E. Quick scan

Answer: B,C,E (LEAVE A REPLY)

FortiClient offers several types of antivirus scans to ensure comprehensive protection:

Full scan: Scans the entire system for malware, including all files and directories.

Custom scan: Allows the user to specify particular files, directories, or drives to be scanned.

Quick scan: Scans the most commonly infected areas of the system, providing a faster scanning option.

These three types of scans provide flexibility and thoroughness in detecting and managing malware threats.

NEW QUESTION: 38

Which statement about FortiClient enterprise management server is true?

A. It provides centralized management of FortiGate devices.

B. It provides centralized management of multiple endpoints running FortiClient software.

C. It provides centralized management of FortiClient Android endpoints only.

D. It provides centralized management of Chromebooks running real-time protection

Answer: B (LEAVE A REPLY)

FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

NEW QUESTION: 39

tiClient behaviour 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.
Answer: A (LEAVE A REPLY)
Action On Virus Discovery Warn the User If a Process Attempts to Access Infected Files Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs.

NEW QUESTION: 40
Which two VPN types can a FortiClient endpoint user inmate from the Windows command prompt? (Choose two)
A. L2TP
B. PPTP
C. IPSec
D. SSL VPN
Answer: C,D (LEAVE A REPLY)
FortiClient supports initiating the following VPN types from the Windows command prompt:
IPSec VPN: FortiClient can establish IPSec VPN connections using command line instructions.
SSL VPN: FortiClient also supports initiating SSL VPN connections from the Windows command prompt.
These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.

NEW QUESTION: 41

Which two statements about ZTNA destinations are true? (Choose two.)
A. FortiClient ZTNA destination encryption is disabled by default.
B. FortiClient ZTNA destinations provides access through TCP forwarding.
C. FortiClient ZTNA destinations do not support a wildcard FQDN.
D. FortiClient ZTNA destination authentication is enabled by default.
E. FottiClient ZTNA destinations use an existing VPN tunnel to create a secure connection.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 42
Refer to the exhibit. You provide a webserver hosting service. An endpoint downloads a test file, testfile.txt, that gets blocked by FortiClient.
Which configuration can you use to make the file accessible on the endpoint?

A. Restore access to file directly using FortiClient.
B. Allow the webserver URL in the exclusion list in the web filter profile.
C. Exclude testfile.txt from the malware protection profile.
D. Add the file to the allowlist in quarantine management on FortiClient EMS.
Answer: D (LEAVE A REPLY)
To allow a specific file that was blocked by FortiClient, the administrator can add it to the allowlist in FortiClient EMS quarantine management. This permits the endpoint to access the file without triggering malware protection.

NEW QUESTION: 43
Which of the following overrides site categories action in FortiClient web-filter?
A. FortiSandbox custom URL categories
B. Block malicious website on AV
C. Web exclusion list
D. URL list
Answer: C (LEAVE A REPLY)
Web exclusion list → explicitly bypasses web filtering. Any URL or domain placed here will override category-based actions and always be allowed.

NEW QUESTION: 44
A security architect has designed a high availability (HA) solution with three FortiClient EMS nodes across two datacenters connected throughsite-to-site IPsec VPN with

1GB of dedicated bandwidth.
How can the architect ensure a seamless failover between FortiClient EMS nodes?
A. License each FortiClient EMS server separately.
B. Provide layer 2 connectivity for the FortiClient EMS servers.
C. Include a remote SQL server in the design.
D. Provide support for active-active HA mode.
Answer: (SHOW ANSWER)
Including a remote SQL server ensures that all FortiClient EMS nodes share a common database. This allows seamless failover between nodes, maintaining consistent endpoint data and configurations across the HA deployment.

NEW QUESTION: 45
A FortiClient EMS administrator has created multiple deployment configurations, and the endpoint is eligible to receive all of them. Which two factors determine which deployment configuration FortiClient EMS applies to the endpoint? (Choose two.)
A. A name of the deployment configuration in alphabetical order.
B. A priority level of the deployment configuration.
C. A status of the deployment configuration.
D. A scheduled time configured on the deployment configuration.
Answer: B,C (LEAVE A REPLY)
When multiple FortiClient EMS deployment configurations could apply to an endpoint:
Priority level → EMS uses the configuration with the highest priority (lower number = higher priority).
Status → Only configurations that are enabled/active are considered. Disabled ones are ignored.

NEW QUESTION: 46
Refer to the exhibit.
FortiClient logs

```
20250226 05:50:24.563 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /
20250226 05:50:24.563 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com
20250226 05:50:24.563 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /
20250226 05:50:24.564 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com / Brave-Dumps.com /
20250226 05:50:24.564 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com / rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.564 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com / Unknown 2025-02-26 05:50:24.564598172
+0100 CET m=+4561.038040408 admin 368039 /opt/google/chrome/chrome}
20250226 05:50:24.601 TZ=+0100 [DEBUG] http2_handler:312 set table size to 65536
20250226 05:50:24.820 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com/favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /favicon.ico
20250226 05:50:24.821 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /favicon.ico Brave-Dumps.com
20250226 05:50:24.821 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com /favicon.ico rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.821 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com /favicon.ico Unknown 2025-02-26 05:50:24.8212255
+0100 CET m=+4561.294667764 admin 368039 /opt/google/chrome
```

Why is the user not able to access bbc.com? (Choose one answer)

A. The URL is blocked by the web filter endpoint profile.

B. The endpoint cannot resolve the URL FQDN.

C. FortiGuard servers are not reachable from the endpoint.

D. The application firewall is blocking Google Chrome.

Answer: C (LEAVE A REPLY)

Based on theFortiClient EMS Administrator Study GuideregardingWeb Filtertroubleshooting and the specific log entries provided in the exhibit, the reason the user cannot access the website is due to connectivity issues with FortiGuard.

1. Analysis of the FortiClient Logs:

* The Error Message:The logs show multiple [ERROR] entries stating: rating_db:97 Category query failure: failed to UrlRequestSendReceive.
* Root Cause Identity:The log explicitly describes the failure: receiveResponse error: FortiGuard server down, task dropped, https bbc.com.
* Resulting Action:Because the endpoint could not receive a rating from the FortiGuard servers, the Web Filter module recorded rating: -1 and applied the action WF_ACTION_BLOCK.

2. Why Option C is Correct:

* FortiGuard Dependency:FortiClient's Web Filter module relies on real-time queries to FortiGuard distribution servers to categorize URLs. If the endpoint is behind a firewall blocking FortiGuard ports (typically UDP 53 or 8888, or HTTPS 443) or has no internet path to these servers, it cannot categorize the site.
* Fail-Safe Behavior:In many FortiClient configurations, if a rating cannot be obtained (Category query failure), the default security posture is to block the request to ensure no potentially malicious or unrated

"Unknown" sites are accessed. The logs confirm this by showing the "FortiGuard server down" message immediately followed by the block action.

3. Why Other Options are Incorrect:

* A. The URL is blocked by the web filter endpoint profile:If it were a standard profile block, the log would show a specificCategory ID(e.g., Category 52 for News and Media) being blocked by policy.

Instead, it shows arating failure (-1).

* B. The endpoint cannot resolve the URL FQDN:The logs show the process correctly identifies host bbc.com. If DNS had failed, the proxy wouldn't even reach the stage of attempting a FortiGuard category query for that specific URL.
* D. The application firewall is blocking Google Chrome:While the log mentions /opt/google/chrome

/chrome, the error is generated by the rating_db and proxy components of the Web Filter, not the Application Firewall module.

NEW QUESTION: 47

Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

A. L2TP

B. PPTP

C. IPSec

D. SSL VPN

Answer: C,D (LEAVE A REPLY)
FortiClient supports initiating the following VPN types from the Windows command prompt:
* IPSec VPN:FortiClient can establish IPSec VPN connections using command line instructions.
* SSL VPN:FortiClient also supports initiating SSL VPN connections from the Windows command prompt.
These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.
References
* FortiClient EMS 7.2 Study Guide, VPN Configuration Section
* Fortinet Documentation on Command Line Options for FortiClient VPN

NEW QUESTION: 48
Which statement about the FortiClient enterprise management server is true?
A. It receives the configuration information of endpoints from ForuGate.
B. It provides centralized management of multiple endpoints running FortiClient software.
C. It enforces compliance on the endpoints using tags
D. It receives the CA certificate from FortiGate to validate client certrficates.
Answer: B (LEAVE A REPLY)
FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

NEW QUESTION: 49
Refer to the exhibit. The zero trust network access (ZTNA) serial number on endpoint br-pc-1 is in a disabled state.
What is causing the problem?

A. The ZTNAfeature is not installed on FortiClient.

B. The ZTNAdestinations endpoint profile is disabled.
C. The ZTNA is disabled due to FortiClient disconnected from FortiClient EMS.
D. The ZTNA certificate has been revoked by administrator.
Answer: C (LEAVE A REPLY)
The ZTNA serial number shows as disabled because FortiClient must maintain a connection with FortiClient EMS for ZTNA functionality. If the client is disconnected or cannot communicate with EMS, the ZTNA serial number will appear disabled.

NEW QUESTION: 50
Which statement about the FortiClient EMS console logs is true?
A. The FortiClient EMS administrator assigned the endpoint profile to All Groups.
B. The FortiClient EMS administrator created an endpoint profile.
C. The FortiClient EMS administrator assigned the gateway list to All Groups.
D. The FortiClient EMS administrator deployed a new FortiClient installation to All Groups.
Answer: (SHOW ANSWER)
This is directly indicated in sample FortiClient EMS questions related to the console logs and endpoint profiles, where the correct choice from similar options is the creation of an endpoint profile by the administrator, not assigning profiles or gateway lists to all groups or deploying new FortiClient installations to all groups.

NEW QUESTION: 51
Refer to the exhibit. An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit.

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

A. The administrator must resolve the XML syntax error.

B. The administrator must use a password to decrypt the file
C. The administrator must change the file size
D. The administrator must save the file as FortiClient-config conf.
Answer: (SHOW ANSWER)
Based on the error message and the XML configuration file shown in the exhibit:
The error "Failed to process the file" typically indicates an issue with the XML syntax.
Upon reviewing the XML content, it is crucial to ensure that all tags are correctly formatted, properly opened and closed, and that there are no syntax errors.
Resolving any XML syntax errors will allow FortiClient to successfully process and restore the configuration file.
Therefore, the administrator must resolve the XML syntax error to fix the issue.

NEW QUESTION: 52
Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

When an administrator creates a deployment profile on FortiClient EMS. which statement about the deployment profile is true?
A. Deployment-2 will upgrade FortiClient on both the AD group and workgroup.
B. Deployment-1 will install FortiClient on new AO group endpoints.
C. Deployment-2 will install FortiClient on both the AD group and workgroup.
D. Deployment-1 will upgrade FortiClient only on the workgroup.
Answer: (SHOW ANSWER)
* Deployment Profiles Analysis:
* Deployment-1 has the "First-Time-Installation" package and is assigned to "All Groups" with a priority of 1 but is not enabled.
* Deployment-2 has the "To-Upgrade" package, is assigned to both "All Groups" and "trainingAD.
training.lab," with a priority of 2 and is enabled.
* Evaluating Deployment-2:
* Deployment-2 will upgrade FortiClient on both "All Groups" and "trainingAD.training.lab" since it is enabled and assigned to these groups. This includes both AD (Active Directory) groups and workgroups.
* Conclusion:
* Since Deployment-2 is set to upgrade FortiClient on all the assigned groups and workgroups, the correct answer is A.
References:
FortiClient EMS deployment and profile documentation from the study guides.

NEW QUESTION: 53
A FortiClient EMS administrator is implementing additional security on FortiClient for compliance checks.
Which tags can the administrator configure to detect endpoints based on vulnerability severity levels?
(Choose one answer)
A. Outbreak alert tags

B. Classification tags
C. Fabric tags
D. Security posture tags
Answer: (SHOW ANSWER)
According to theFortiClient EMS 7.2/7.4 Administration Guideand theZTNA Deployment Guide, the administrator can configureSecurity posture tags(also known asZero Trust Network Access (ZTNA) tags in recent versions) to detect and group endpoints based on specific compliance criteria, including vulnerability severity levels.
1. How Security Posture Tags Work for Vulnerabilities:
* Tagging Rules: Under theSecurity Posture Tags(orZero Trust Tags) section in EMS, an administrator creates a new rule set and adds a rule.
* Rule Type: The administrator selects theVulnerable Devicesrule type.
* Severity Levels: Within this rule, the administrator can specify theSeverity Level(such asCritical,High
,Medium, orLow). EMS dynamically applies the tag to any endpoint where the vulnerability scan detects at least one vulnerability matching or exceeding that severity level.
* Dynamic Grouping: These tags allow for dynamic grouping of endpoints, which can then be synchronized with a FortiGate to enforce access control based on the device's current security posture.
2. Why Other Options are Incorrect:
* A. Outbreak alert tags: While FortiGuard Outbreak alerts can be used in tagging, they specifically target endpoints vulnerable to a particular "outbreak" or high-profile threat currently active in the wild, rather than providing a general mechanism for all vulnerability severity levels.
* B. Classification tags: These tags are typically used for broader endpoint identification (like department or location) and sending information to FortiAnalyzer for reporting, rather than real-time security posture compliance based on vulnerability scans.
* C. Fabric tags: "Fabric" usually refers to the integration between Fortinet devices (the Security Fabric).
While tags are shared across the Fabric, the specific tags configuredwithinEMS for endpoint detection based on posture are categorized as Security Posture/Zero Trust tags.
3. Curriculum References:
* FortiClient EMS Administration Guide (Zero Trust Tagging Rules section): Explicitly details the
"Vulnerable Devices" rule type and its severity options.
* EMS Study Guide (Compliance & Vulnerability): Describes using these tags to ensure endpoints meet minimum security standards before being granted access to the network.

NEW QUESTION: 54
Which two statements are true about the ZTNA rule? (Choose two.)
A. It applies security profiles to protect traffic
B. It applies SNAT to protect traffic.
C. It defines the access proxy.
D. It enforces access control.
Answer: (SHOW ANSWER)
Understanding ZTNA Rule Configuration:
The ZTNA rule configuration shown in the exhibit defines how traffic is managed and controlled based on specific tags and conditions.
Evaluating Rule Components:
The rule includes security profiles to protect traffic by applying various security checks (A).
The rule also enforces access control by determining which endpoints can access the specified resources based on the ZTNA tag (D).
Eliminating Incorrect Options:

SNAT (Source Network Address Translation) is not mentioned as part of this ZTNA rule.
The rule does not define the access proxy but uses it to enforce access control.
Conclusion:
The correct statements about the ZTNA rule are that it applies security profiles to protect traffic (A) and enforces access control (D).

NEW QUESTION: 55
An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient. What must the administrator do to achieve this requirement?
A. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
B. Disable select the vulnerability scan feature in the deployment package
C. Click the hide icon on the vulnerability scan profile assigned to endpoint
D. Use the default endpoint profile
Answer: (SHOW ANSWER)
* Requirement Analysis:
* The administrator needs to maintain a software vulnerability scan on endpoints without showing the feature on FortiClient.
* Evaluating Options:
* Disabling the feature in the deployment package or endpoint profile would remove the functionality entirely, which is not desired.
* Using the default endpoint profile may not meet the specific requirement of hiding the feature.
* Clicking the hide icon on the vulnerability scan profile assigned to the endpoint will keep the feature active but hidden from the user's view.
* Conclusion:
* The correct action is to click the hide icon on the vulnerability scan profile assigned to the endpoint (C).
References:
FortiClient EMS feature configuration and management documentation from the study guides.

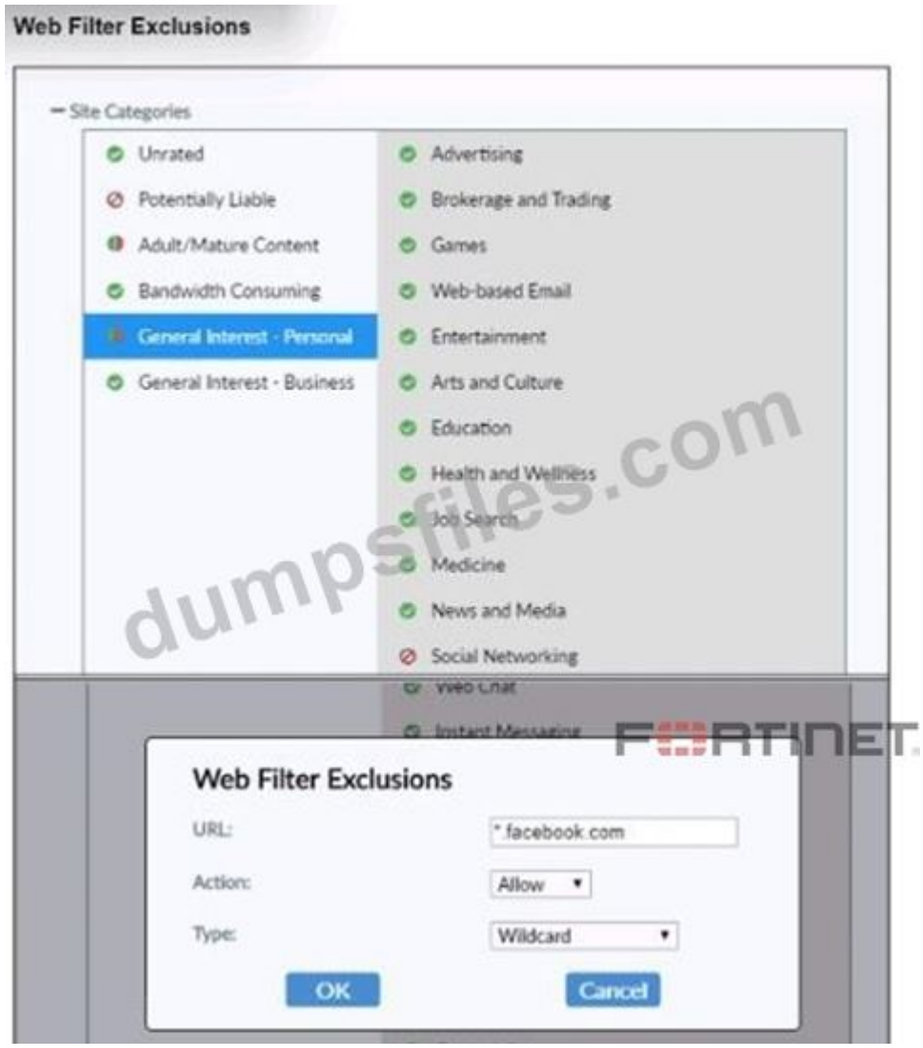
NEW QUESTION: 56
An administrator must add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.
Which solution can provide secure access between FortiClient EMS and the Active Directory server?
A. Configure and deploy a FortiGate device between FortiClient EMS and the Active Directory server.
B. Configure Active Directory and install FortiClient EMS on the same VM.
C. Configure a slave FortiClient EMS on a virtual machine.
D. Configure an Active Directory connector between FortiClient EMS and the Active Directory server.
Answer: A (LEAVE A REPLY)
* Requirement:
* The administrator needs to add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.
* Solution Analysis:
* The goal is to securely connect FortiClient EMS and the Active Directory server despite being in different security zones.
* Evaluating Options:
* Installing FortiClient EMS on the same VM as Active Directory (option B) is not practical due to security zone separation.
* Configuring a slave FortiClient EMS on a virtual machine (option C) does not address the need for secure communication.
* Configuring an Active Directory connector (option D) may not be sufficient without secure routing.
* Conclusion:

* Deploying a FortiGate device between FortiClient EMS and the Active Directory server ensures secure and controlled access between the two zones.
References:
FortiClient EMS and FortiGate configuration and deployment documentation from the study guides.

NEW QUESTION: 57
Which Fortinet solution can you integrate FortiClient with to use the single sign-on mobility agent (SSOMA) feature?
A. FortiAuthenticator
B. FortiSASE
C. FortiPAM
D. FortiNAC
Answer: A (LEAVE A REPLY)
FortiClient integrates with FortiAuthenticator to use the SSOMA feature, enabling single sign-on for endpoint users and providing seamless authentication for network access.

NEW QUESTION: 58
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
Answer: (SHOW ANSWER)
* Understanding Compliance Rules:
* The compliance rule for the sales department needs to be enforced dynamically.
* Enforcing Compliance:
* FortiGate is responsible for enforcing compliance by integrating with FortiClient EMS to apply dynamic access control based on compliance status.
* Conclusion:
* The Fortinet device that will enforce compliance with dynamic access control is the FortiGate.
References:
Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

NEW QUESTION: 59
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?

A. FortiClient will allow access to Facebook.

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

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

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

Answer: (SHOW ANSWER)

* Observation of Web Filter Exclusions:

* The exhibit shows a web filter exclusion for "*.facebook.com" with the action set to "Allow."

* Evaluating Actions:

* This configuration means that FortiClient will allow access to Facebook and its subdomains.

* Conclusion:

* When users try to access "www.facebook.com," FortiClient will allow the access based on the web filter exclusion settings.

References:

FortiClient web filter configuration and exclusion documentation from the study guides.

NEW QUESTION: 60

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

A. Import and verify the FortiClient EMS tool CA certificate on FortiGate.

B. Revoke and update the FortiClient client certificate on EMS.
C. Import and verify the FortiClient client certificate on FortiGate.
D. Revoke and update the FortiClient EMS root CA.
Answer: A (LEAVE A REPLY)
* Connecting FortiClient EMS to FortiGate:
* The administrator needs to establish a connection between FortiClient EMS and FortiGate as a fabric connector.
* Prerequisites for Connection:
* A key prerequisite is the import and verification of the FortiClient EMS tool CA certificate on FortiGate to ensure a trusted connection.
* Conclusion:
* The correct prerequisite for a successful connection is to import and verify the FortiClient EMS tool CA certificate on FortiGate.
References:
FortiClient EMS and FortiGate connection and certificate management documentation from the study guides.

NEW QUESTION: 61
Refer to the exhibit. Based on the CLI output from FortiGate. which statement is true?

A. FortiGate is configured to pull user groups from FortiClient EMS
B. FortiGate is configured with local user group
C. FortiGate is configured to pull user groups from FortiAuthenticator
D. FortiGate is configured to pull user groups from AD Server.
Answer: A (LEAVE A REPLY)
Based on the CLI output from FortiGate:
The configuration shows the use of "type fortiems," indicating that FortiGate is set up to interact with FortiClient EMS.
The "server" field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.
The configuration includes an SSL-enabled connection, which is a common setup for secure communication between FortiGate and FortiClient EMS.
Thus, the configuration indicates that FortiGate is set up to pull user groups from FortiClient EMS.

Valid FCP_FCT_AD-7.4 Dumps shared by TrainingDump.com for Helping Passing FCP_FCT_AD-7.4 Exam! TrainingDump.com now offer the **newest FCP_FCT_AD-7.4 exam dumps**, the TrainingDump.com FCP_FCT_AD-7.4 exam **questions have been updated** and **answers have been corrected** get the