Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

NEW QUESTION 1
Which statement about sending notifications with incident updates is true?

A. Each connector used can have different notification settings
B. Each incident can send notification to a single external platform.
C. You must configure an output profile to send notifications by email.
D. Notifications can be sent only when an incident is created oi deleted.

Answer: A

NEW QUESTION 2
Aplaybook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails.
What will be the status of the playbook after it is run?

A. Attention required
B. Upstream_failed
C. Failed
D. Success

Answer: A

Explanation:
In FortiAnalyzer, when a playbook is run, each task??s status impacts the overall playbook status. Here??s what happens based on task outcomes:
* Status When All Tasks Succeed:
* If all tasks finish successfully, the playbook status ismarked asSuccess.
* Status When Some Tasks Fail:
* If one or more tasks in the playbook fail, but others succeed, the playbook status generally changes toAttention required. This status indicates that the playbook completed execution but requires review due to one or more tasks failing.
* This is different from a completeFailedstatus, which is used if the playbook cannot proceed due to a critical error in an early task, often one that upstream tasks depend on.
* Option Analysis:
* A. Attention required: This is correct as the playbook has completed, but with partial success and a task requiring review.
* B. Upstream_failed: This status is used if a task cannot run because a prerequisite or "upstream" task failed. Since four out of five tasks completed, this is not the case here.
* C. Failed: This status would imply that the playbook completely failed, which does not match the scenario where only one task out of five failed.
* D. Success: This status would apply if all tasks had completed successfully, which is not the case here.
Conclusion:
* Correct Answer A. Attention required
* The playbook status reflects that it completed, but an error occurred in one of the tasks, prompting the administrator to review the failed task.
References:
FortiAnalyzer 7.4.1documentation on playbook execution statuses and task error handling.

NEW QUESTION 3
You mustfind a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been uncuccessful.
Which two tasks should you perform to investigate why you are having this issue? (Choose two.)

A. Open .gz log files in FortiView.
B. Rebuild the SQL database and check FortiView.
C. Review the ADOM data policy
D. Check logs in the Log Browse

Answer: AB

NEW QUESTION 4
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. FortiView Monitor
B. Outbreak alert services
C. Incidentsdashboard
D. Threat hunting

Answer: D

Explanation:
FortiAnalyzer offers several features for monitoring, alerting, and incident management, each serving different purposes. Let's examine each option to determine which one best supports a proactive security approach.
* Option A - FortiView Monitor:
* FortiView is a visualization tool that provides real-time and historical insights into network traffic, threats, and logs. While it gives visibility into network activity, it is generally more reactive than proactive, as it relies on existing log data and incidents.
* Conclusion:Incorrect.
* Option B - Outbreak Alert Services:
* Outbreak Alert Services in FortiAnalyzer notify administrators of emerging threats and outbreaks based on FortiGuard intelligence. This is beneficial for awareness of potential threats but does not offer a hands-on, investigative approach. It??s more of a notification service rather than an active, proactive investigation tool.
* Conclusion:Incorrect.
* Option C - Incidents Dashboard:
* The Incidents Dashboard provides a summary of incidents and current security statuses within the network. While it assists with ongoing incident response, it is used to manage and track existing incidents rather than proactively identifying new threats.

* Conclusion:Incorrect.
* Option D - Threat Hunting:
* Threat Hunting in FortiAnalyzer enables security analysts to actively search for hidden threats or malicious activities within the network by leveraging historical data, analytics, and intelligence. This is a proactive approach as it allows analysts to seek out threats before they escalate into incidents.
* Conclusion:Correct.Conclusion:
* Correct Answer D. Threat hunting
* Threat hunting is the most proactive feature among the options, as it involves actively searching for threatswithin the network rather than reacting to already detected incidents.
References:
FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

NEW QUESTION 5
What are the two methods you can use to send notifications when an event is generated by an event handler? (Choose two answers)

A. Send SNMP trap.
B. Send an alert through the FortiGuard server.
C. Send an alert through Fabric connectors.
D. Send SMS notification

Answer: AC

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer event handlers support alerting when a rule match generates an event. The study guide states that, for an event handler,??You can select a notification profile to send alerts whenever an event is generated by the handler.??In FortiAnalyzer, notification profiles are the mechanism used to deliver alerts outward (for example, via an SNMP trap), which directly aligns with optionA.
In addition, FortiAnalyzer supports sending notifications to external platforms through integrations:??You can configure FortiAnalyzer to send a notification to external platforms using preconfigured Fabric connectors.??This validates the use ofFabric connectorsas a notification delivery method, aligning with optionC.
OptionBis not a notification delivery method for event-handler-generated alerts in the workflow described (FortiGuard is used for threat intelligence/enrichment rather than relaying alerts). OptionDis not presented in the study guide??s described notification mechanisms for event-handler alerting in the referenced sections.

NEW QUESTION 6
Which statement about automation connectors in FortiAnalyzer is true?

A. An ADOM with the Fabric type comes with multiple connectors configured.
B. The local connector becomes available after you configured any external connector.
C. The local connector becomes available after you connectors are displayed.
D. The actions available with FortiOS connectors are determined by automation rules configured on FortiGate.

Answer: D

NEW QUESTION 7
In a FortiAnalyzer Fabric deployment, which three modules from Fabric members are available for analysis on the supervisor? (Choose three answers))

A. Playbooks
B. Indicators
C. Logs
D. Events
E. Reports

Answer: CDE

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The study guide explicitly describes what content fromFabric membersis visible/usable on theFabric supervisor:
* Logs:??In the FortiAnalyzer Fabric supervisor,Log View displays logs collected on all FortiAnalyzer Fabric members.??
* Reports:??For reports, the FortiAnalyzer Fabric supervisorcan fetch and aggregate data from multiple membersin the FortiAnalyzer Fabric.??
* Events:??Events generated by event handlers on the FortiAnalyzer Fabric members are visible on the supervisor.??
By contrast, the study guide lists a key limitation that rules outPlaybooksas a supervisor capability over members: ??You are not able to perform configuration changes or torun automation playbooks from the Fabric supervisor to members.??
Therefore, the three modules available for analysis on the supervisor areLogs, Events, and Reports(C, D, E).

NEW QUESTION 8
Refer to the exhibit with partial output:

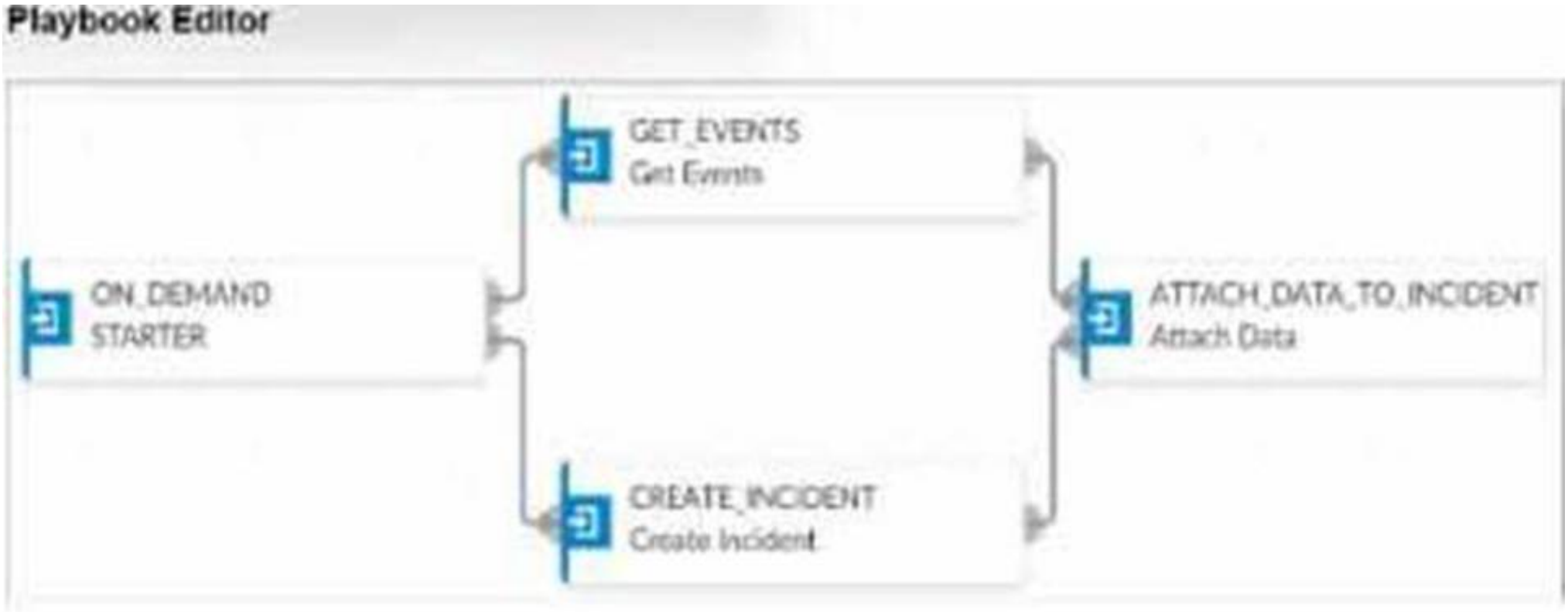
Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

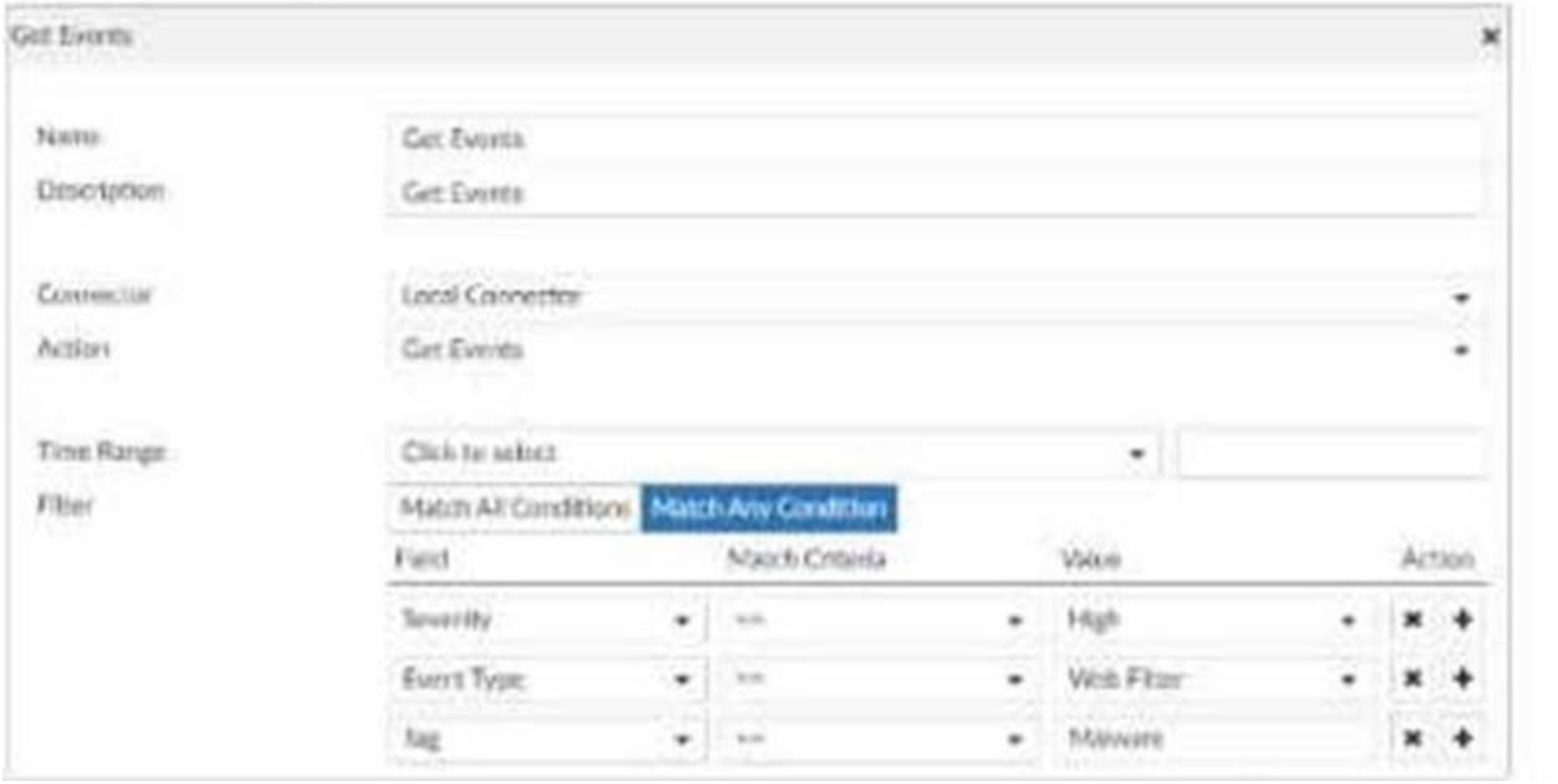
A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

Answer: A

Explanation:
In the exhibit, the data structure shows a checksum field and a data field with a long, seemingly encoded string. This format is indicative of a file that has been compressed or encoded for storage and transfer.
Export Data Type:
The data field is likely a base64-encoded string, which is commonly used to represent binary data in text format. Base64 encoding is often applied to data that has been compressed (zipped) for easier handling and transfer. The checksum field, with an MD5 hash, provides a way to verify the integrity of the data after decompression.
Option Analysis:
* A. The export data type is zipped: Correct. The compressed and encoded format of the data suggests that the export is in a zipped format, allowing for efficient storage and transfer.
* B. The playbook is misconfigured: There is no indication of misconfiguration in this exhibit. The presence of the checksum and data fields aligns with standard export practices.
* C. The option to include the connector was not selected: There is no evidence in the output to conclude that connectors are missing. Connectors are typically listed separately and would not directly affect the checksum and encoded data structure.
* D. Your colleague put a password on the export: There??s no indication of password protection in the exhibit. Password protection would likely alter the data structure, and there would be some mention of encryption.
Conclusion:
Correct Answer:A. The export data type is zipped.
This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.
[References:, FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.,]

NEW QUESTION 9
Exhibit.





Assume these are all the events that exist on the FortiAnalyzer device.
How many events will be added to the incident created after running this playbook?

A. Eleven events will be added.

B. Seven events will beadded
C. No events will be added.
D. Four events will be added.

Answer: D

Explanation:
In the exhibit, we see a playbook in FortiAnalyzer designed to retrieve events based on specific criteria, create an incident, and attach relevant data to that incident. The "Get Event" task configuration specifies filters to match any of the following conditions:
Severity= High
Event Type= Web Filter
Tag= Malware
Analysis of Events:
In the FortiAnalyzer Event Monitor list:
We need to identify events that meet any one of the specified conditions (since the filter is set to "Match Any Condition").
Events Matching Criteria:
Severity = High:
There are two events with "High" severity, both with the "Event Type" IPS.
Event Type = Web Filter:
There are two events with the "Event Type" Web Filter. One has a "Medium" severity, and the other has a "Low" severity.
Tag = Malware:
There are two events tagged with "Malware," both with the "Event Type" Antivirus and "Medium" severity.
After filtering based on these criteria, there arefour distinct events:
Two from the "Severity = High" filter.
One from the "Event Type = Web Filter" filter.
One from the "Tag = Malware" filter.
Conclusion:
Correct Answer:D. Four events will be added.
This answer matches the conditions set in the playbook filter configuration and the events listed in the Event Monitor.
[References:, FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident management criteria.,]

NEW QUESTION 10
In firmware version 7.6, how does on-premises FortiAnalyzer store logs? (Choose one answer)

A. Uses ClickHouse database
B. Uses MySQL database
C. Uses Postgres SQL database
D. Uses ElasticSeach database

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer 7.6 stores on-premises logs in aClickHouse SQL database(not MySQL, Postgres, or Elasticsearch). Fortinet??s FortiAnalyzer 7.6 SQL Query documentation explicitly states that log data is inserted into the SQL database and that "FortiAnalyzer uses a ClickHouse SQL database."
This is consistent with how the study guide describes the storage/analytics pipeline in 7.6: it explains that FortiAnalyzer indexes incoming raw logs (insert rate)"by the SQL database and the sqlplugind daemon." This "SQL database" in 7.6 corresponds to the ClickHouse-backed log database described in the Fortinet documentation.

NEW QUESTION 10
How does FortiAnalyzer block indicators? (Choose one answer))

A. It uses an automation script to update FortiGate with the block list.
B. It uses a FortiManager connector to send the block list.
C. It uses a FortiClient EMS connector to send the block list.
D. It uses a webhook to allow FortiGate to send the block list.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The FortiAnalyzer study guide states that blocking suspicious indicators is performed by integrating FortiAnalyzer withFortiManager(not by directly pushing a block list to FortiGate). Specifically:"To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the Fabric Connector page of FortiAnalyzer."
It then explains the backend mechanism:"In the back end, a playbook called Block_indicator runs every 5 minutes to send the information to FortiManager."After a successful run,"the blocked indicator is pushed to the FortiManager External Resource list."From there, FortiManager can create threat feeds/security profiles/policy blocks and push policies to FortiGate as needed—however, the study guide clarifies:??The Blocked status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.??
Therefore, FortiAnalyzer blocks indicators by using aFortiManager connectorand sending the block information to FortiManager (Option B).

NEW QUESTION 11
Refer to the exhibit.

```
adom_oid=198 itime=2025-05-27 08:35:24 loguid=7509149554218893312 epid=3 euid=3 data_parsername=FortiGate Log Parser data_sourceid=FGVM02TM24013423
data_sourcename=HQ-NGFW-1 root data_sourcetype=FortiGate data_timestamp=1748334923 app_cat=unscanned app_name=NTP app_service=NTP dst_intf=port2(undefined)
dst_ip=208.91.112.63 dst_port=123 event_action=accept event_id=13 event_policy=3 event_ref=751261e0-ce9e-51ef-f12e-a382acaf16d6 event_severity=notice
event_subtype=forward event_type=traffic host_location=Reserved host_owner=fortinet.com net_proto=17 net_rcvdpkts=1 net_rcvbytes=76 net_sentbytes=76 net_sentpkts=1
net_sessionduration=180 net_sessionid=1357 src_intf=port6(undefined) src_ip=10.0.13.125 src_natip=100.65.0.101 src_natport=50403 src_port=50403 dstepid=101 dsteuid=3
dst_geo_country=United States event_creation_time=27800868 event_uuid=0000000013 src_geo_country=Reserved logflag=1 data_sourcedom=root dst_intf_role=undefined
event_policyid=3 event_policytype=policy src_intf_role=undefined itime_t=1748360124 _logMeta=undefined
```

Which two observations can you make after reviewing this log entry? (Choose two answers))

A. This is a normalized log.
B. This is a formatted view of the log.
C. This is the original log that FortiAnalyzer received from FortiGate.
D. This log is in a raw log format.

Answer: AD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The exhibit shows the log as a single-line key/value entry (not a columnar/table display), which aligns with FortiAnalyzer'sraw log formatview option. The study guide states:"You can toggle between viewing formatted and raw logs."This directly supports observationD.
At the same time, what you are viewing in FortiAnalyzer Log View isnormalizeddata (FortiAnalyzer parses and maps device logs into standardized fields for consistent searching and analysis). The study guide explicitly states:"The log view allows you to view all log types received by FortiAnalyzer in normalized log format.??It also explains that FortiAnalyzer "uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names," then stores them as normalized logs in the SIEM database. This supports observationA.
Finally, the study guide clarifies that even when you switch to raw log format in FortiAnalyzer, you are still observing the normalized-field representation produced by FortiAnalyzer's parser/normalization process (rather than the untouched original device message). It notes that a FortiGate event log "has been normalized by FortiAnalyzer," and when you switch "to raw log format," you can observe the effect of normalization on common fields. This is whyCis not the best description for the exhibit.

NEW QUESTION 15
Which log will generate an event with the status Contained?

A. An AV log with action=quarantine.
B. An IPS log with action=pass.
C. A WebFilter log will action=dropped.
D. An AppControl log with action=blocked.

Answer: A

NEW QUESTION 16
When there are no matching parsers for a device log, what does FortiAnalyzer do? (Choose one answer))

A. Drops the log
B. Applies the generic SYSLOG parser
C. Stores the log but doesn't normalize it
D. Archives the log for future analysis

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer's ingestion pipeline does not "drop" logs simply because a parser is unavailable. The study guide states that when devices send logs,"Logs received are decompressed and saved in a log file on the FortiAnalyzer disk??(with a .log extension). This establishes that the raw log is still accepted and stored on disk as part of the normal workflow.
Normalization, however, depends on having a suitable parser. The study guide explains that "FortiAnalyzer uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names."It further emphasizes that??Log parsers ?? are central to log normalization" because they convert unstructured/native logs into a standardized schema.
Therefore, ifno matching parserexists for a given device log, FortiAnalyzer can stillstore the incoming log(it is received, decompressed, and written to disk), but it cannot perform the "extract key fields" and "map to standardized field names" steps required for normalization. In practical terms, the log remains in its native/unstructured form (not normalized), which aligns exactly with optionC.

NEW QUESTION 19
You need to move reports between two ADOMs.
Which two statements are true? (Choose two.)
A. The ADOMs must be compatible types.
B. The date and time will be appended to the original report name to avoid conflicts.
C. All charts and datasets associated with the report will be imported together.
D. You need to convert the reports into templates first.

A.

Answer: AC

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer supports moving reporting content across ADOMs by importing/exporting reporting objects, but it enforces ADOM compatibility. The study guide states: "You can, however, import and export reports and charts ... into different ADOMs ..." and explicitly requires that "Both ADOMs must be of the same type." This directly validates statement A.
For report dependencies, the study guide clarifies how datasets are handled during transfer. While "You can't export templates and datasets," it also explains that when you export a chart, "the associated dataset is exported with it, so when you import an exported chart, the associated dataset is imported as well." Since reports are composed of charts (and charts depend on datasets), moving a report between ADOMs entails moving its charts; when those charts are exported/imported, their datasets come with them. This supports statement C based on the documented chartdataset import/export behavior.
Statement D is not required because the study guide explicitly indicates you can "export and import reports" directly, and additionally notes that on import "you can save the layout of the report as a template" (optional, not a prerequisite).

NEW QUESTION 24
Which statement regarding macros on FortiAnalyzer is true?

A. Macros are predefined templates for reports and cannot be customized.
B. Macros are useful in generating excel log files automatically based on the report settings.
C. Macros are ADOM-specific and each ADOM type have unique macros relevant to that ADOM.
D. Macros are supported only on the FortiGate ADOMs.

A.

Answer: B

Explanation:
Macros in FortiAnalyzer are used to streamline reporting tasks by automating data extraction and report generation. Here's a breakdown of each option to determine the correct answer:
Option A - Macros are Predefined Templates for Reports and Cannot be Customized:
This statement is incorrect. Macros in FortiAnalyzer are not simply fixed templates; they allow for customization to tailor data extraction and reporting based on specific needs and configurations.
Conclusion: Incorrect.
Option B - Macros are Useful in Generating Excel Log Files Automatically Based on the Report Settings:
This statement is accurate. Macros in FortiAnalyzer can be configured to automate the generation of reports, including outputting log data to Excel format based on predefined report settings. This makes them especially useful for scheduled reporting and data analysis.
Conclusion: Correct.
Option C - Macros are ADOM-Specific and Each ADOM Type Has Unique Macros Relevant to that ADOM:
Macros are not limited to specific ADOMs, nor are they ADOM-specific. Macros can be applied across various ADOMs based on report configurations but are not inherently tied to or unique for each ADOM type.
Conclusion: Incorrect.
Option D - Macros are Supported Only on the FortiGate ADOMs:
This is not true. Macros in FortiAnalyzer are not restricted to FortiGate ADOMs; they can be utilized across different ADOMs that FortiAnalyzer manages.
Conclusion: Incorrect.Conclusion:
Correct Answer B. Macros are useful in generating excel log files automatically based on the report settings.
This answer correctly describes the functionality of macros in FortiAnalyzer, emphasizing their role in automating report generation, especially for Excel log files.
FortiAnalyzer 7.4.1 documentation on macros and report generation functionalities.

NEW QUESTION 27
Which statement about SQL SELECT queries is true?

A. They can be used to purge log entries from the database.
They must be followed immediately by a WHERE clause.
B. They can be used to display the database schema.
C. They are not used in macros.
D.

Answer: D

Explanation:
Option A - Purging Log Entries:
A SELECT query in SQL is used to retrieve data from a database and does not have the capability to delete or purge log entries. Purging logs typically requires a DELETE or TRUNCATE command.
Conclusion: Incorrect.
Option B - WHERE Clause Requirement:
In SQL, a SELECT query does not require a WHERE clause. The WHERE clause is optional and is used only when filtering results. A SELECT query can be executed without it, meaning this statement is false.
Conclusion: Incorrect.
Option C - Displaying Database Schema:
A SELECT query retrieves data from specified tables, but it is not used to display the structure or schema of the database. Commands like DESCRIBE, SHOW TABLES, or SHOW COLUMNS are typically used to view schema information.
Conclusion: Incorrect.
Option D - Usage in Macros:
FortiAnalyzer and similar systems often use macros for automated functions or specific query-based tasks. SELECT queries are typically not included in macros because macros focus on procedural or repetitive actions, rather than simple data retrieval.
Conclusion: Correct.
Conclusion:
Correct Answer D They are not used in macros.
This aligns with typical SQL usage and the specific functionalities of FortiAnalyzer.
Reference: FortiAnalyzer 7.4.1 documentation on SQL queries, database operations, and macro usage

NEW QUESTION 30
Which log will generate an event with the status Unhandled?

An AV log with action=quarantine.
A. An IPS log with action=pass.
B. A WebFilter log will action=dropped.
C. An AppControl log with action=blocked.
D.

Answer: B

Explanation:
In FortiOS 7.4.1 and FortiAnalyzer 7.4.1, the "Unhandled" status in logs typically signifies that the FortiGate encountered a security event but did not take any specific action to block or alter it. This usually occurs in the context of Intrusion Prevention System (IPS) logs.
IPS logs with action=pass: When the IPS engine inspects traffic and determines that it does not match any known attack signatures or violate any configured policies, it assigns the action "pass". Since no action is taken to block or modify this traffic, the status is logged as "Unhandled."

Let's look at why the other options are incorrect:
An AV log with action=quarantine: Antivirus (AV) logs with the action "quarantine" indicate that a file was detected as malicious and moved to quarantine. This is a definitive action, so the status wouldn't be "Unhandled."
A WebFilter log will action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.
An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

NEW QUESTION 31
Which statement describes archive logs on FortiAnalyzer?

A. Logs that are indexed and stored in the SQL database
B. Logs a FortiAnalyzer administrator can access in FortiView
C. Logs compressed and saved in files with the .gz extension
D. Logs previously collected from devices that are offline

Answer: C

Explanation:
In FortiAnalyzer, archive logs refer to logs that have been compressed and stored to save space. This process involves compressing the raw log files into the .gz format, which is a common compression format used in Fortinet systems for archived data. Archiving is essential in FortiAnalyzer to optimize storage and manage long-term retention of logs without impacting performance.
Let's examine each option for clarity:
Option A: Logs that are indexed and stored in the SQL database
This is incorrect. While some logs are indexed and stored in an SQL database for quick access and searchability, these are not classified as archive logs. Archived logs are typically moved out of the database and compressed.
Option B: Logs a FortiAnalyzer administrator can access in FortiView
This is incorrect because FortiView primarily accesses logs that are active and indexed, not archived logs. Archived logs are stored for long-term retention but are not readily available for immediate analysis in FortiView.
Option C: Logs compressed and saved in files with the .gz extension
This is correct. Archive logs on FortiAnalyzer are stored in compressed .gz files to reduce space usage. This archived format is used for logs that are no longer immediately needed in the SQL database but are retained for historical or compliance purposes.
Option D: Logs previously collected from devices that are offline
This is incorrect. Although archived logs may include data from devices that are no longer online, this is not a defining characteristic of archive logs.
Reference: FortiAnalyzer 7.4.1 documentation and configuration guides outline that archived logs are stored in compressed files with the .gz extension to conserve storage space, ensuring FortiAnalyzer can handle a larger volume of logs over extended periods?.

NEW QUESTION 33
Refer to the exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 78.8, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

What can you conclude about the output?

A. The low indexing values require investigation.
B. The output is not ADOM specific.
C. There are more event logs thantraffic logs.
D. The log rate higher than the message rate is not normal.

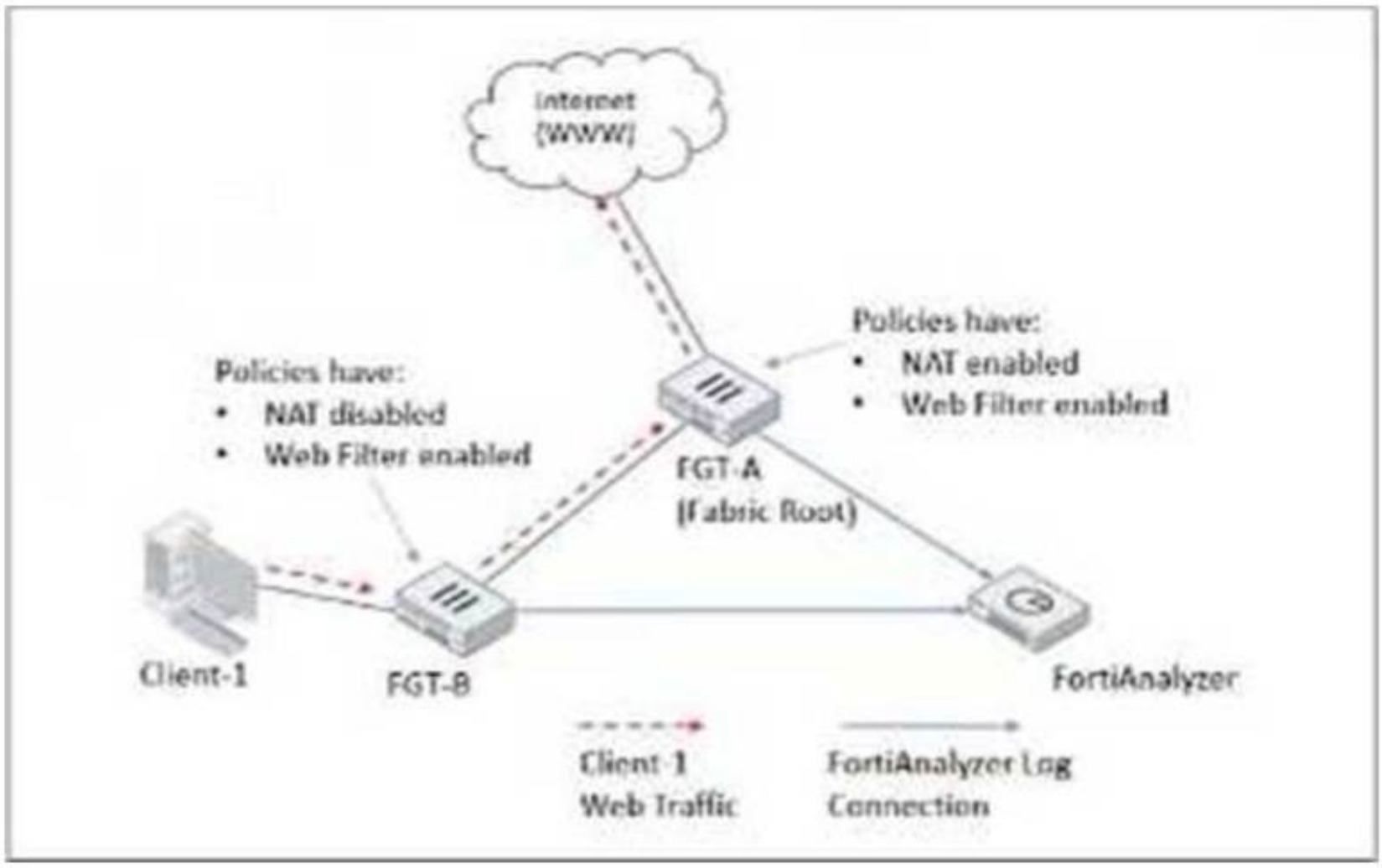
Answer: D

NEW QUESTION 38
Which two parameters does FortiAnalyzer use to identify an indicator of compromise (IOC)? (Choose two answers)

A. IP address
B. URL
C. Policy ID
D. Application category

Answer: AB

NEW QUESTION 40
Refer to Exhibit:



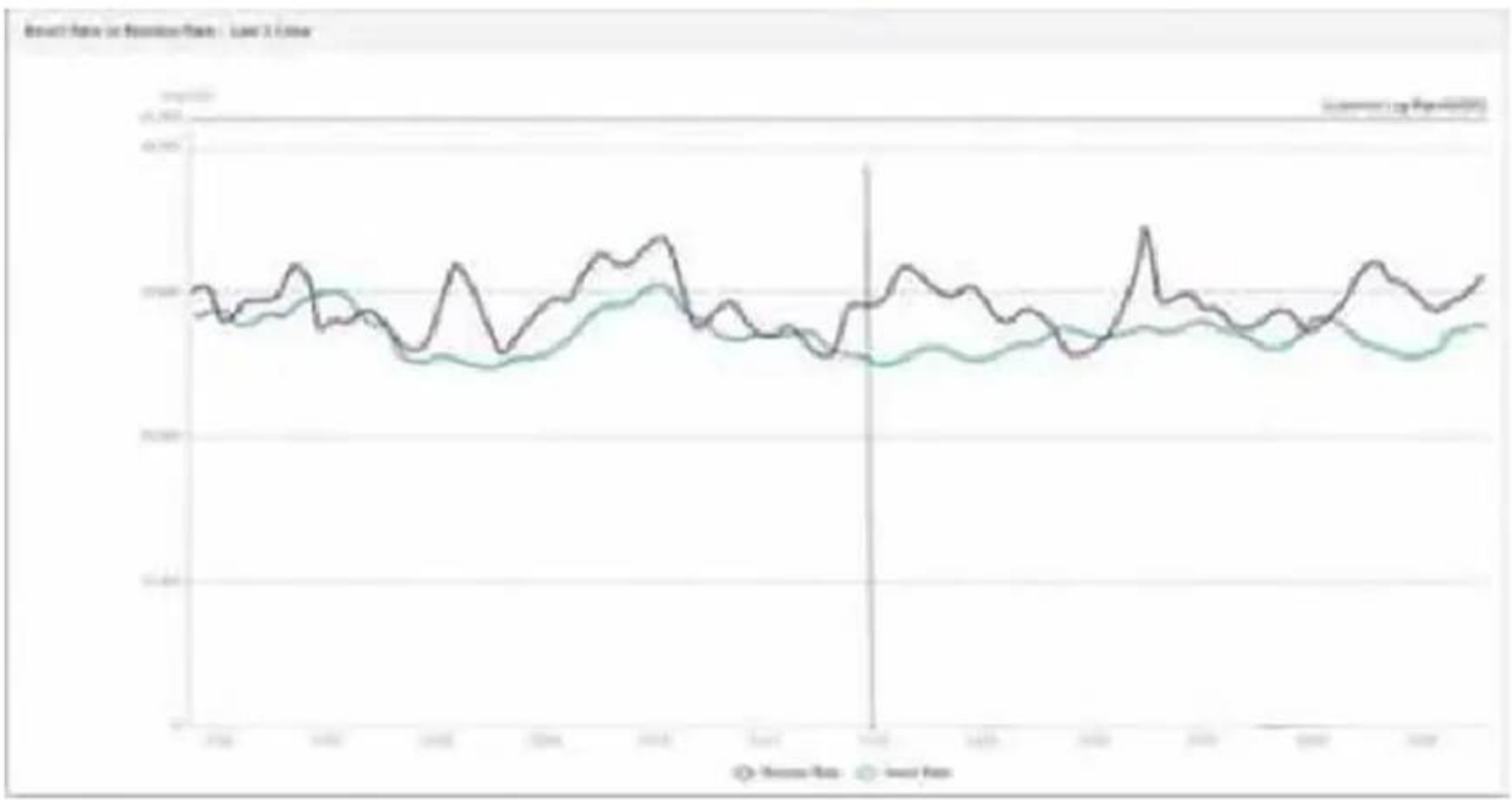
Client-1 is trying to access the internet for web browsing.
All FortiGate devices in the topology are part of a Security Fabric with logging to FortiAnalyzer configured. All firewall policies have logging enabled. All web filter profiles are configured to log only violations.
Which statement about the logging behavior for this specific traffic flow is true?

A. Only FGT-B will create traffic logs.
B. FGT-B will see the MAC address of FGT-A as the destination and notifies FGT-A to log this flow.
C. FGT B will create traffic logs and will create web filter logs if it detects a violation.
D. Only FGT-A will create web filter logs if it detects a violation.

Answer: D

Explanation:
The study guide explains that in a Security Fabric,traffic logging is not duplicatedacross FortiGates for the same session:??Traffic logging for a session ?? is always carried out by the first FortiGate that handled it??and if a FortiGate receives traffic from a peer FortiGate MAC,"it does not generate a new traffic log for that session."
For UTM (web filtering) logs, the study guide states:"When configured, upstream devices complete UTM logging."
In the illustrated example, it further clarifies the role split:"All traffic from Client-1 is first received by FGT-B, which creates traffic logs for the initial session?? [then] forwarded to FGT-A?? [and]FGT-A ?? applies web filtering ?? and generates the relevant UTM logs as necessary."
Because web filter profiles are configured tolog only violations, web filter (UTM) logs will be generated only when a violation is detected—and per the study guide behavior, that UTM logging is done by theupstreamFortiGate (FGT-A). Therefore,only FGT-A will create web filter logs if it detects a violation(Option D)

NEW QUESTION 42
Exhibit.



What does the data point at 12:20 indicate?

A. The loginsert log time is increasing.
B. FortiAnalyzer is using its cache to avoid dropping logs.
C. The performance of FortiAnalyzer is below the baseline.
D. The sqiplugind service is caught up with the logs

Answer: A

NEW QUESTION 43
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: AC

NEW QUESTION 44
A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL
B. IPSec
C. Direct serial connection
D. S/MIME

Answer: B

NEW QUESTION 47
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FAZ_AN-7.6 Practice Exam Features:

* FCP_FAZ_AN-7.6 Questions and Answers Updated Frequently

* FCP_FAZ_AN-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AN-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AN-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year